REFEDS

REFEDS Fall Meeting 2011 – Minutes

Licia Florio and Nicole Harris

Abstract:

Minutes of the REFEDS Fall Meeting 2011 held in Helsinki, Finland on 14th September 2011 in conjunction with IRISC.

Table of Contents

1. Welcome and REFEDS Updates (Licia Florio)

1.1 Agenda bashing.

No changes to the agenda were proposed.

1.2 Last meeting minutes approval and related actions.

The Boundary Router proposal has been subsumed in to the work for Moonshot so this will not be taken forward as a REFEDS workitem.

David Simonsen (DS) proposed a slight change to the terms of REFEDS to make it more explicit how project proposals should be brought to REFEDS and approved. Licia Florio (LF) will present on this later in the meeting and update the website appropriately.

1.3 Reports, budget for Y2 and next meetings.

An end of year report has been sent to the sponsors and LF will circulate to the whole list shortly.

ACTION20110914-01: LF to circulate REFEDS end of year report to REFEDS list.

LF described the established approach for starting a work item within REFEDS. Any REFEDS member may present a short plan to the list with budget, timeframe, outputs and how this relates to the REFEDS plan and direction. The group will discuss the proposals on the mailing list. If the plan gains support on the list, it will be taken to the Steering Committee.

Thomas Legenhagger (TL) asked that proposals should be longer and more detailed than we have seen so far. This could be done by having a 2-phase approach, with specifications presented first and then more details about the project management later.

LF confirmed that the budget for year 1 had been spent as proposed.

LF presented the new REFEDS plan and noted that the Steering Committee had approved the change of financial planning from an August – July year to a calendar year.

New activities that have already been approved are updates to the website, a new blog for REFEDS and REFEDS sessions at Internet2 and APAN are being planned. The blog has not been implemented as yet as TERENA support staff members have little time and do not have the experience of federating blogs. Several participants offered support in making this work effectively.

ACTION20110914-02: Leif Johansson to talk to LF and Nicole Harris (NH) about setting up a federated blogging platform for REFEDS.

It has been proposed by the Steering Committee that REFEDS should think more closely about how we work with other groups. We are beginning this process by ensuring REFEDS sessions are globally accessible with sessions at both Internet2 and APAN in 2011/12.

Chris Phillips (CP) proposed that REFEDS should write to ORCID as a follow up to the IRISC meeting with some proposals about how our work might interact. Most of the work focused on interfederation work cases and potential for carrying ORCID identifiers.

ACTION0110914-03: CP and NH to work on a set of bullets that can be worked up in to a REFEDS response to ORCID as a meeting follow-up.

The participants agreed that it is necessary for REFEDS to have a presence internationally and approved travel to these events to host REFEDS BOFS / meetings.

2. REFEDS2 Barriers to Effective Federation Use (Nicole Harris)

NH presented the proposed outputs under the REFEDS2 work item. As these areas have been extensively discussed at previous REFEDS meetings this item was predominantly to verify actions, approaches and timescales.

The Discovery work will involve the creation of a toolkit; Nicole has already identified a potential firm that could carry out the design work, however she invited the audience to come forward with alternative firms. DS noted that the toolkit should not be targeting publishers only, but general SPs. It was noted that it's easier to start with publishers just because both Nicole and Rod have already contacts with them.

ACTION0110914-04: Identify other immediate target audience for the toolkit.

NH and Rod Widdowson are seeking volunteers to work on the Discovery project editorial board. All REFEDS participants are invited to take part.

The other work item in REF2 is the Barrier for SP document and its updates.

A discussion followed and the main question was how many federations would be willing to change their policies; there seems to be consensus that policies can be changed and simplified and it was agreed that it should be the ID Fed goal to improve the policies.

Maybe REFEDS and this work item in particular should make recommendations on how policies could be simplified.

3. REFEDS3 Boundary Solutions (David Simonsen)

The meeting attendees ware asked to consider the proxy proposals put forward by David Simonsen (DS) and Diego Lopez (DL). The Steering Committee was not able to

make a decisions on whether to take these forward so asked the group to make a decision on whether the projects should be taken forward. Two main issues were identified with the proposals, namely that ezproxies are commercial tools and that ezproxies encourage the usage of IP-based access, which is not considered a good practise.

CP asked if Wondertool be developed to become an appropriate tool? It was generally agreed that this would not be the right base to work from.

(i) WAYF proposal: this work is aimed at those users that manage/configure EZproxy that is administrative people and those in charge of licenses to indicate that a service is available for an institution. The idea is to develop a Web GUI to access the EZproxies.

The added value for the federations would be that the proxies would become SPs; the users would then login to the proxy via the federation.
This solution would also allow integrating services (that is the proxies) that are not planning to implement federated access (maybe because the software do not support SAML and may not be web-based).

(ii) RedIRIS proposal: The proposal is to create a repository accessed and controlled by the federation to manage the configuration rules for the proxy. The configuration rules can be written for both Ezproxies and apache proxies (RedIRIS is running the latter). This means that the configuration is outsourced to the federations.

DS explained that the core benefit would be for administrators within institutions, although it was recognised that this role was carried out be several different role types within a typical federation. The core benefit for the federations would be the increased in service providers within the federation.

Although EZProxy has a publisher focus, this approach could be used in more use cases where IP is almost exclusively used, bringing a wider benefit beyond the library scenario.

Leif Johansson compared the configuration information being centrally collated in DL's model to the role that saml metadata plays within federations. Could this configuration process be standardised to the level of the SAML approach? CP asked about the role of OCLC – we have identified a need and an output that meets this need; he also proposed to work more closely with OCLC to make this happen in a more balanced way, especially considering that OCLC has a shibolised version of the EZProxy.

Milan Sova (MS) and Lalla questioned the value of the proxy process for federations – is this an institutionally focused service only?

A long discussion followed, the conclusion of which was that still it was not clear for some of the participants why institutions that run proxies would be interested in the federation, and this should be considered an institutional SSO problem not a federation problem. The counter argument to this was that the proposals would enable replacing IP-based login with federated login and in this case the institutions running the proxies would become member of the federations.

4

Options for taking this forward:

- Approve the projects;
- Approve only one of two project and evaluate the benefits;
- Merge the 2 proposals in to 1 project;
- Take the proposals to OCLC as REFEDS;
- Further articulate the projects.

It was agreed that the proposals are not fundable as they are at this moment; a discussion with OCLC will take place and the two proposals will be re-scoped and maybe merged into one. However it was agreed that this area should be maintained within the REFEDS workplan, and that there was no clear dissent for the work within the group, more a misunderstanding and lack of understanding regarding requirements.

ACTION20110914-05: NH to arrange a meeting between REFEDS and OCLC to further discuss the proxy proposals. The re-scoped proposals will be then sent to the SC for approval.

4. REF5 Inter-federation - PEER (Leif Johansson)

LJ gave a brief background overview of the PEER project. The software is available for testing. At the moment, there is enough interest in PEER to mean there will be several instances running; this does not mean that there will be more instance for REFEDS, but only that different user-communities will run an instance. The sustainability of service instances and the sustainability of the software are being addressed by the 3rd phase of the project.

The PEER process was demoed by Lorenzo Gil from Yaco, the software developers.

Questions from the floor:

- *Will the login be federated?*

Yes, but we will need to deal with multiple login approaches as SPs may not have an IdP to use in this way.

- *How does a federation use this information?*

An instance of PEER will deliver a signed saml metadata aggregator. It is up to the federation what it then does with the information that has been consumed (separate, all in etc.). Different federations are bound to approach this differently.

- *Will PEER allow filtering of data at the PEER interface?*

Yes this will be possible in future instances.

- *Who will host the public instance of PEER?*

Possible homes are ISOC and REFEDS.   It is likely that we stand something up as peer.refeds.org in this first instance with VM hosting by Nordunet. Leif is preparing a business case around this.

- *Will there be multiple instances of PEER?*

The PEER software can be used in many different ways, for example by federations who currently want to improve their metadata management tools. However we aim to have a single public instance that will be used by REFEDS organisations.

LJ explained that PEER is only intended to provide a central registrar for metadata, it does not replace any other functionality / vetting currently undertaken by federations.

ACTION20110914-06: Send feature requests for PEER and / or PEER questions to the PEER list (peer@refeds.org) or to LJ directly.

5. Business Models for Federations in an Interfederation Environment (Nicole Harris)

NH outlined the potential business implications and impacts of interfederation on federation funding models. There are a variety of potential impacts ranging from lack of income from Service Providers who choose to only join one federation to increased overhead for federations that do not charge membership.

Participants agreed that federations should follow a pragmatic approach in considering business model impact. There are a variety of models beyond 'membership' that could be used to ensure that Service Providers contribute to the cost of federation operations. Suggestions included:

- Not charging SPs to join but charging them for support.
- Charging to add to an interfederation aggregation but not for local access.

It was agreed that a watching brief should be kept on this area (as part of REF5) and that REFEDS could add value by documenting requirements that could be presented to appropriate federation boards.

ACTION20110914-07: Add a watching brief on the impact of inter-federation on the federations' business model.

6. REF6 Levels of Assurance (Leif Johansson)

6.1 LEGO

LJ began the discussion by looking at what the motivation might be to increase LOA within federations and the concepts behind the LEGO work item. A clear example is PubMed[1], which requires FICAM LOA1.

LJ started from the point of view that any federation should be able to pass an LOA1 accreditation and for some federations even LOA2. Looking at matching an LOA1 requirement to federation policies would be a good place to start before we attempt to do something more specific with LOA.

---

1 http://www.ncbi.nlm.nih.gov/pubmed/

To date there are two global groups looking at LOA that are of direct relevance to REFEDS, Kantara and OIX. Kantara LoA work is mostly focused on LOA 2 and 3 whilst OIX is focused on LOA1 at this point in time.

The OIX trust framework is a set of requirements (listed in a doc); OIX would accredit the federation operators as trusted introducers, meaning that the federation would then be able to introduce the list of IdPs into OIX. The business model is still unclear – and it is unknown whether each IdPs that becomes OIX accredited would be charged a fee in an accredited federation model.

SWAMID have started the process of mapping the SWAMID policy to the OIX requirements; two potential issues were identified, namely the high value insurance required by the profile and some too US-centric requirements. NH has also carried this out with the UK federation policy and will add this information to the wiki.

Diego Lopez asked if it would be worth EU entities becoming OIX accredited; Leif noted that there is a possibility for European entities to apply for US funding that where LOA is required by a service.

- *What's the difference between InCommon Silver and OIX profile?*
A: InCommon silver is not OIX accredited yet, however the requirements between the two profiles of them are the same.

- *How does this relate to the EU data protection?*
A: federations in EU have to comply with them anyway, but it's certainly something to discuss on the LEGO list.

- *How about the opt-in requirement?*
A: there is room to modify this.

ACTION20110914-08: NH to upload UK mapping to LEGO workspace on to the REFEDS the wiki.

6.2 IRISC and LOA

Mikael Linden (ML) gave a report back from the IRISC meeting. ML invited participants to attend a meeting at STFC in the UK on the 2nd-3rd November 2011[2] to take these discussions further. From the IRISC meeting, ML noted that researchers were not using federations due to lack of attribute information and lack of attribute release policies being established.

Face-to-face identity proofing was identified as one of the core requirements in terms of assurance from the researchers involved in the meeting. This is close to a NIST definition of LOA2. Accountability is another requirement, and it is important that accounts belong to individuals.

In principle InCommon Silver and Bronze would fulfil the requirements of the eScience community, although they seem too US-Centric and their internationalization would require

---

[2] This meeting is the follow up of the meeting held at CERN in the summer.

considerable levels of work.

6.3 Other LOA Activities

Chris Brown (CB) and Heath Marks (HM) gave an update on the approaches to LOA from the JISC and AAF perspective. HM outlined a problem well recognised in many institutions – the processes to reach a higher LOA simply aren't in place within institutions.

It is important for federations to find an effective point to start when defining LOA requirements. Participants agreed that the IGTF vetting processes were not a good model to review.

7. REF4 Attribute Release Recommendations (Steven Carmody)

Steven Carmody (SC) presented the work of the attribute release sub-group of REFEDS. This group has been working on a set of recommendations around good practice for attribute release for approximately 6 weeks and had prepared an early set of findings for REFEDS to consider and refine.

Core shift in thinking from the group included a focus on considering all attributes as potentially personally identifiable information (PII) and a change in the way 'necessary' was defined from an association with 'being able to complete work / study' to 'being able to access without barriers' (minimal disclosure use case).

The group has structured a set of recommendations in different areas:
- Policy framework;
- Approaches that simplify the management of attribute release policies;
- GUI recommendations for consent / informing;
- SAML 2 metadata recommendations.

Participants discussed the best approach for summarising this information and for communicating it to federations. Along with the Barriers to SPs work, this will be one of the first direct approaches to federations by REFEDS.

An important result was that the federations represented at the meeting unanimously voted yes to the question "Would you, as a Federation operator, support sending the GUI recommendations to the SAML software projects, and ask them to develop implementations as soon as possible? "

The final report from this group is expected in Jan 2012.

ACTION20110914-09: SC, NH and LF to discuss format and communication channels for the outputs of the attribute release work.

8. Coordinating the cloud services

Ken Klingestein (KK) reported that I2 is in the process of signing a contract with box.net at reduced rates. The service would be available to students and faculties (no alumni); the service will be enabled via InCommon.

KK reported on the some of the issues found:

- How do you describe a service that is enabled by the federation?
- Many of the commercial SPS do not understand multi-layered federation;
- At least in the box.net case, there was a high interest in groups and groups APIs; in US groups are considered part of the federations; there was consensus among the participants that groups are important elements of federations.
- Attribute release policies: campuses will be agreeing to the release policy.

LJ reported on the progress made by SUNET to procure a cloud service for their community. One of the options to reduce the price is the possibility of offering capacity to the cloud provider. LJ noted that in Europe there are only a few NRENs that can offer capacity to the US. Some of the attendees however felt the capacity was not a showstopper for a joint procurement.

In the context of REFEDS it was agreed to discuss attribute mappings and any other policies that would be playing a role when procuring a cloud service.

ACTION20110914-10: Establish a brief watch on attribute coordination when federating new services.

9. Action Summary

Action Reference	Action Summary	Action Assignment
20110914-01	Circulate REFEDS end of year report to REFEDS list.	Done
20110914-02	Discuss and action setting up a federated blogging platform for REFEDS.	LF, NH and LJ
20110914-03	Work on a set of bullets to become REFEDS response to ORCID as a meeting follow-up.	CP and NH
20110914-04	Identify other immediate target audience for the toolkit (REF2)	NH
20110914-05	Arrange a meeting between REFEDS and OCLC to further discuss the proxy proposals.	NH
20110914-06	Send feature requests for PEER and / or PEER questions to the PEER list (peer@refeds.org) or to LJ directly.	ALL
20110914-07	Add a watching brief on the impact of inter-federation on the federations' business model.	LC, NH

20110914-08	Upload UK mapping to LEGO workspace on to the REFEDS the wiki.	NH
20110914-09	Discuss format and communication channels for the outputs of the attribute release work.	SC, LF and NH
20110914-10	Establish a brief watch on attribute coordination when federating new services (REF2 or REF4?)	NH, LC

10. Online Participants (13)

Andreas Solberg
Bob Morgan, Internet2
David Chadwick, Univ. of Kent
Glenn Wearen, eduGate
Heather Flanagan, Internet2
Keith Hazleton, Internet2
Ken Klingenstein, Internet2
Klaas Wierengam CISCO Systems
Maarten, SURFnet
Mark Williams, JISC Collections
Niels Van Dijk, SURFnet
Steven Carmody, Internet2
Steve Moitozo
Victoriano Giralt, Univ. Malaga
Ingrid Melve, UNINETT

11. Participants in Helsinki (31)

Sabita Behari SURFnet
Christopher Brown JISC (CB)
Licia Florio TERENA (LF)
Lorenzo Gil Yaco
Hideaki Goto NII Japan
Nicole Harris JISC Advance (NH)
Leif Johansson NORDUnet/SUNET (LJ)
Kari Laalo CSC
Janne Lauros CSC
Thomas Lenggenhager SWITCH (TL)
Mikael Linden CSC (ML)
Diego Lopez RedIRIS (DL)
Lucy Lynch Internet Society
Lalla Mantovani IDEM (GARR) / IT
Heath Marks Australian Access Federation (HM)
Timo Mustonen CSC
Valter Nordh NORDUnet / GU
Kari Nousiainen Ubisecure Solutions Inc.
Pascal Panneels BELNET
Chris Phillips CANARIE Inc. (CP)

Michal Prochazka CESNET
Alex Reid AARNet
Brook Schofield TERENA
Sami Silén CSC
David Simonsen WAYF
Milan Sova CESNET (MS)
Hannes Tschofenig Nokia Siemens Networks
Keith Uber Ubisecure Solutions
Hildegunn Vada UNINETT
Pieter van der Meulen SURFnet
Joost van Dijk SURFnet