REFEDS

REFEDS MINUTES, MAY 2014

LICIA FLORIO AND NICOLE HARRIS

Abstract:

Chairs: Nicole Harris (morning session) and Licia Florio (afternoon session)

Nicole welcomed attendees to the meeting and noted that 83 attendees were signed up to the meeting. A full list of participants can be found here: https://eventr.terena.org/events/1926.

Several people were attending REFEDS for the first time. All presentations from the meeting will be published at: https://refeds.org/meetings/may14/.

1. Introduction, Licia Florio.

Licia gave a brief overview of the REFEDS developments since the last meeting and against the 2014 workplan. The main achievements so far in 2014 include:

- First REFEDS Entity Category approved and published;
- Federation Operators Practice (FOP) progressed: first document out for comments;
- Updated version of the metadata explorer tool (MET) released.

Licia noted that the sponsorship for 2014 is not finalised yet, but this is a critical issue towards the implementation of the work plan. For 2015, some REFEDS work will be funded via GEANT4 and the Horizon 2020 calls where there are clear synergies.

2. Ian Young, Metadata Query Protocol and SAML Entity Metadata Attribute Type.

Ian presented two documents that are currently being passed through the RFC process as REFEDS drafts:

- Metadata Query Protocol;
- The Entity Category SAML Entity Metadata Attribute Type.

These are being identified as REFEDS documents via boilerplate text in the Independent Stream as per discussions in previous REFEDS meetings.

ACTION20140518-01: Participants were asked to comment on the boilerplate text being used in the RFCs and suggest appropriate amendments. The text can be found in Ian's slides or in the submitted RFCs.

The Entity Category SAML Entity Metadata Attribute Type has been published for several years via the mace-dir group, but at this time was purposefully not published via the RFC process.. The mace-dir group has agreed that it is now appropriate to publish via this process given the uptake of Entity Categories by REFEDS and individual federations.

ACTION20140518-02: Nicole Harris to issue a 4 week comment and consultation period for the Entity Category SAML Entity Metadata Attribute Type draft.

The Metadata Query Protocol is very similar to DNS Query. It is not a language or attribute algebra system but a simple, REST-like access protocol at the moment.

Participants asked if REEP could return different metadata for different requestors. There are no plans for this at the moment and further discussions would be needed to understand the use case. Chris Phillips suggested the following SP as an example:

https://met.refeds.org/met/met/entity/https%253A%252F%252Fe5.onthehub.com/.

Ian asked for scrutiny by possible implementers at this stage to ensure that the protocol has been scoped appropriately. New features are not being requested at this time. Specific areas for scrutiny include caching / GET issues.

3. Service Updates, Leif Johansson, Nicole Harris and Licia Florio

3.1 REEP / PEER Updates

http://reep.refeds.org

Leif gave an update on the REEP service and underlying PEER service developments. A focus for PEER has been improving the SAML Metadata Editor tool to enhance the experience of using the tool as well as general bug fixing and improvements.

For REEP, the focus has been on the underlying service infrastructure and trust management architecture - which will be very important in the context of REEP. Focus has also been given to REEP policy, integration with SAMLbits and use of the Metadata Query Protocol work.

In terms of moving to service delivery, Steve O from ISOC is working on material to communicate the importance of REEP to publishers. Other important user groups will then be tackled - this work is primarily advertising / marketing work on top of the service.

ACTION20140518-03: REFEDS Coordinators to contact the CZ Atlas SP to ask if they would be interested in publishing via REEP.

ACTION20140518-04: REFEDS Coordinators to talk to Steve O about materials for Service Providers.

The REEP signing process was ideally to take place in Stockholm but it was logistically difficult. There will be a video published to show the initialization of the HSM environment and that was a witness auditor when the all process was done in Stockholm. A key signing ceremony for REEP will be held after the REFEDS meeting.

It was noted that at the moment eduGAIN does not consume REEP metadata and is unable to as it only accepts metadata from federations. These issues will be explored further in GN4 if the current project plans are accepted.

REEP is purposefully limited to research and education entities. Consideration should be given to whether eScience related entities should be included in REEP or in a separate PEER instance.

3.2 MET updates

http://met.refeds.org/met/

The Metatada Explorer Tool gives high level management information on the number of entities that are in a federations and where entities appear in multiple federations. Some simple stats can be derived to support management reporting. MET could be taken forward to include much more detailed analysis, but further work should only be carried out if this offers value.

MET is currently only on a test server and needs to be moved to a full production environment. Work on the current version of MET was carried out by DAASI.

ACTION20140518-05: Nicole Harris to discuss hosting arrangements for MET with Nordunet and DAASI.

More discussion on statistical information from federations is needed. David Simonsen explained Kantara's interest in this area.

ACTION20140518-06: REFEDS Coordinators to seek further feedback for future MET developments.

3.3 SCHAC updates

SCHAC started as a TF-EMC2 project but has not been actively maintained for some time. Licia Florio has proposed a workplan to update SCHAC. The Initial work will be funded by TERENA as a small project. This work will cover:

- Review of the existing SCHAC documentation: decision on which URN to use (urn:mace:terena.org:schac was deprecated in 2011 in favour of urn:schac);
- SCHAC attribute definition page should be updated (currently on line at: http://www.terena.org/registry/terena.org/attribute-def/) to list OID instead than URN

- Move all existing documentation (SCHAC specifications PDF and SCHAC LDAP Schema) into **one single authoritative SCHAC specification** containing all the necessary information.
- Create a SCHAC editorial board.

Work will be carried out in the last quarter of 2014.

4. Federation Operators Update

4.1 Federation Operators Group (FOG) Updates

Peter Schober gave an update on the Federation Operators Group (FOG) 1 year after its inception. The group is working well and has proven to be a useful addition to the REFEDS environment. There could be more discussion on exchanging information and expertise and to distill more "best practices" in the future inline with the FOP work (see below).

Niels van Dijk raised the issue that it was currently difficult to find out what development plans other federations had at any given point, which would be useful when considering developments within your own federation. REFEDS has in the past collated some information via wiki pages, but it is difficult to incentivise people to keep the pages up-to-date.

Nicole proposed that a short, well-focused, annual survey could be a more useful approach with information published via the REFEDS website. This should have some relationship with the TERENA Compendium but should be completed by Fed Op staff. Attendees agreed that such an approach would be welcomed.

ACTION20140518-06: REFEDS Coordinators to draft and plan an annual federation survey.

4.2 Federation Operator Practice (FOP) Update

Nicole gave an overview and explained the motivations for the FOP work. REFEDS received clear feedback from the FIM4R group was that it's difficult to find out working processes followed by different federations and as such fully understand the trust model that was in place. With the rise of inter-federation, the question of how different federations processes match each other becomes more important.

The FOP work is initially scope as 4 practice statements and the first (Metadata Registration Practice Statement) is now out in first draft for comment. After this meeting there will be a formal 4 weeks consultation period.

ACTION20140518-07: Nicole Harris to launch a 4 week consultation period for the Metadata Registration Practice Statement.

5. Trust and Identity Coordination among European NRENs, Valter Nordh

Valter reported on the EU effort to coordinate work on AAI. Valter mentioned the newly formed committee TIC (Trust and Identity Committee) to help inform a strategy for NRENs in the EU. Valter noted that it could be an opportunity for REFEDS to get some of the results to management attention.

The following input was given as to what the TIC could do:

- We have too much work to do with the number of people we have available.
- We need the TIC to be in the room at REFEDS and other events.
- Influence the managers on our behalf and promote the work of REFEDS.
- Internship capability for people coming out of school to work on our projects, with a committed amount of time before they disappear off to Google. Distinguished engineer / REFEDS school? We have the skilled staff to help teach them.

6. Interfederation is real - what can REFEDS do to help?

6.1 Code of Conduct

Mikael gave an update on progress with adoption of the code of conduct and monitoring tools being used within eduGAIN. For the international Code of Conduct, the lawyer has indicated that ink signatures may be required. This was cause scalability issues that would make this impossible to proceed with.

Attendees asked about the relationship between the CoC and other entity categories (e.g. R&S). It was confirmed that federations are using the categories together to support attribute release.

The REFEDS Coordinators confirmed that to name the international Code of Conduct the "REFEDS Code of Conduct" will need to go through the REFEDS Steering Committee process for approval if it were to be named in this way.

ACTION20140518-08: Mikael Linden to send out a final call for comments on the International Code of Conduct.

ACTION20140518-09: REFEDS SC to consider the implications of using the name "REFEDS Code of Conduct".

6.2 Entity Categories

Nicole reported on progress with the Entity Categories work. The main use-case for this is for IdPs to release a set of attributes to services that fall into certain categories that have been pre-vetted by authorities such as federation operators. The Research and Scholarship Entity Category has now been published and is ready for use.

Attendees asked how entity category work can be properly promoted. The work should be pushed forward by individual federations; however there may be a value on providing general information that federations may use. Nicole has started an FAQ document on the wiki for this purpose.

Nicole presented discussion so far on 2 new Entity Categories:

- Hide from discovery: there were no particular concerns about the scope of this category, although some federations would not have specific use cases for it. It was agreed that this category should be pushed forward for consultation.

- "library" entity category: the conversation on the mailing list derailed into an LOA discussion; however NH will summarise the part of the conversation that relates to this category.

ACTION20140518-10: Nicole Harris to issue 4 week comment period on "hide from discovery" entity category.

ACTION20140518-11: Nicole Harris to summarise discussions on affiliation / library entity categories on the REFEDS wiki.

Another area that has been discussed is the idea of a category for affiliation. Niels van Dijk and Leif Johansson have drafted a specification of an alternative broker service approach to proving "studentness" and will share this specification with this list.

ACTION20140518-12: Niels van Dijk to share specification for "studentness" validation service with REFEDS list.

6.3 eduGAIN Update

Brook looked at the problems of starting with only theoretical use cases rather than real use cases when developing architectures and policies and the issues with killing them off as our infrastructure grows.

An identified problem that has emerged as part of the interfederation effort is that RequestedAttribute not being populated effectively, meaning SPs cannot rely on consistent attribute release from different countries. Attribute bundles via entity categories are supposed to address this but until they are effectively managed we have to rely on Requested Attribute.

The Knodium example has been discussed on the eduGAIN list. Once you put the metadata out in the wild, strange things start to happen; a more elegant solution is needed to this problem. RequestedAttribute works well locally but does not scale in the way intended within interfederation.

ACTION20140518-13: REFEDS Coordinators to establish a working group to discuss a solution to managing attribute expression in interfederation use-

cases. Ken volunteered to chair this group and work with the REFEDS Coordinators to set up the appropriate infrastructure. Tentatively named: managing attribute requirements inter-federation (mari).

7. K-12 Session

Ken Klingenstein gave a brief overview of the problems facing federations that wish to extent an offering to schools. Many federations are now either connecting schools or are in discussion as to how this can be achieved.

There will be a lunchtime session during TNC14 to discuss this further. It is expected that an output of this discussion will be to request a specialist working group list to be set up under the banner of REFEDS to discuss issues in this space. This is turn may lead to formal work item requests for REFEDS in the future.

8. Attribute Authorities

Kristof Bajnok gave an update on the Attribute Authority Collaboration work being carried out as part of the GEANT project. This includes the HEXAA project (funded as part of the GEANT Open Calls), the GEANT Research Activity work, and work by Perun.

9. FedLab and REFEDS

Roland Hedberg gave an overview of the work being carried out in GEANT and beyond to create robust monitoring and testing tools for SAML and OpenID Connect. The purpose of this tool is to help entities joining federation achieve a suitable standard of interoperability.

This work now needs to move beyond the research activity phase, and there is interest from both Kantara and the OpenID Foundation in supporting such a tool. It is proposed that REFEDS participates in this work.

ACTION20140518-14: Licia Florio to work with Roland Hedberg to create a plan on FedLab and REFEDS for REFEDS SC approval.

10. Everything as service / Open Floor

The final session of the day offered an “open-mic” opportunity for REFEDS participants to give updates, with a focus on out-of-the-box service models within federations.

- Lalla Mantovani reported on GARR’s plan to run ‘federation as a service”, following the IdP in the cloud approach.
- Ken Klingenstein report on the improved version on uApprove being developed by Internet2.
- Marina Vermezovic: asked participants for advice on where to find a list of the most popular SPs? This maybe something to add to the

REFEDS survey? NH suggested that MET might help here.

- Niels van Dijk gave a brief overview of the "studentness" verification service specification (https://wiki.surfnet.nl/display/SvS/RFC%3A+Simple+Validation+Service).

11. ACTION Summary:

Item	Description	Assigned To
ACTION20140518-01	Comment on the boilerplate text being used in the RFCs and suggest appropriate amendments. The text can be found in Ian's slides or in the submitted RFCs.	ALL
ACTION20140518-02	Issue a 4 week comment and consultation period for the Entity Category SAML Entity Metadata Attribute Type draft.	Nicole Harris
ACTION20140518-03	Contact the CZ Atlas SP to ask if they would be interested in publishing via REEP.	REFEDS Coordinators
ACTION20140518-04	Talk to Steve O about materials for Service Providers.	REFEDS Coordinators
ACTION20140518-05	Discuss hosting arrangements for MET with Nordunet and DAASI.	Nicole Harris
ACTION20140518-06	Draft and plan an annual federation survey.	REFEDS Coordinators
ACTION20140518-07	Launch a 4 week consultation period for the Metadata Registration Practice Statement.	Nicole Harris
ACTION20140518-08	Final call for comments on the International Code of Conduct.	Mikael Linden
ACTION20140518-09	Consider the implications of using the name "REFEDS Code of Conduct".	REFEDS SC
ACTION20140518-10	Issue 4 week comment period on "hide from discovery" entity category.	Nicole Harris
ACTION20140518-11	Summarise discussions on affiliation / library entity categories on the REFEDS wiki.	Nicole Harris

ACTION20140518-12	Share specification for “studentness” validation service with REFEDS list.	Niels van Dijk
ACTION20140518-13	Establish a working group to discuss a solution to managing attribute expression in interfederation use-cases. Ken volunteered to chair this group and work with the REFEDS Coordinators to set up the appropriate infrastructure. Tentatively named: managing attribute requirements inter-federation (mari).	REFEDS Coordinators
ACTION20140518-14	Work with Roland Hedberg to create a plan on FedLab and REFEDS for REFEDS SC approval.	Licia Florio