REFEDS

REFEDS Participant Meeting – Minutes Maastricht, June 2013

Licia Florio and Nicole Harris

Table of Contents

1. Welcome and Introductions 2
2. REF13-1: REFEDS RFC Stream 2
3. REF13-2: International Code of Conduct 2
4. REF13-2: Entity Categories and Certification Marks 3
5. REF13-2: Baseline Assurance within Federations 3
7. REF13-4: REEP Update 4
8. REF13-4: MET: Metadata Explorer Tool 5
9. Shibboleth Consortium Update 5
10. New Proposal: Update on SCHAC 5
11. Federation as a Service 5
12. PERUN: User and Resource Management System 6
13. SAML Test Harness project 6
14. SUNET Update 6
15. Federation Operators Forum Proposal 6
16. NSTIC Update 7

1. Welcome and Introductions

Licia Florio welcomed participants to the meeting, and advised that she had circulated update slides on current status of the REFEDS workplan and budget to the REFEDS list but did not intend to present them.

Participants were invited to review the REFEDS Participant's Agreement and remind themselves of the terms under which REFEDS operates. The new Steering Committee members were also welcomed.

Licia noted that this was the first REFEDS meeting without Milan Sova, and participants were invited to remember him and his contributions to our work.

2. REF13-1: REFEDS RFC Stream

Nicole Harris gave a brief update on the work to create an Independent RFC Stream for REFEDS. An RFC describing how this might work has been completed and REFEDS is now awaiting further discussion within the RFC community. Nicole will attend IETF in Berlin (July 2013) where further discussions will be held.

Possible candidate documents for this RFC stream are the mace-dir work on Entity Categories, the Code of Conduct, and the MDX work (which is currently published as an Individual submission). Should it prove difficult to agree on an Independent Stream for REFEDS, it is likely that we will continue to use the Individual Stream.

Participants asked if REFEDS could do more to look at creating external promotional documents to help explain some of our processes to typical institutions. It was agreed that this should be examined.

ACTION20130602-01: Nicole Harris to discuss promotional materials with TERENA PR team.

3. REF13-2: International Code of Conduct

Mikael Linden gave an update on the work carried out to create the Code of Conduct. The Code of Conduct is a pilot Entity Category that allows Service Providers to declare they have signed up to a certain set of criteria around data protection and data handling.

A pilot of the Code of Conduct was carried out with the CLARIN community during 2013. Voting is now open to include the Code of Conduct in eduGAIN via the Technical Steering Group - members of eduGAIN were asked to use their vote.

Ken Klingenstein asked how this would function in the wider space of multiple entity categories. It was agreed that it would be necessary to have multiple entity tags for individual entities.

Mikael confirmed that the Code of Conduct is self-asserted, so there is no need to renew it each year or carry out specific audit steps.

Next steps for the Code of Conduct will be:

- To submit the Code of Conduct to the Article 29 working party.
- To look at an international code of conduct beyond Europe.
- To extend the Code of Conduc to allow the release of optional extra attributes.

Participants asked if it was possible for the Code of Conduct to be combined with Safe Harbour? This is already possible under the current Code of Conduct but it was noted that Universities are outside of the Safe Harbour agreement.

Entity Categories should be able to work out of the box with Shibboleth 2.4 release.

4. REF13-2: Entity Categories and Certification Marks

Ken Klingenstein gave a background to the problems that end users have in managing their privacy and presented certification marks as a concept to try and make this easier for typical users to understand. Certification marks would be auditing and verified marks with a recognizable graphic for users to trust, similar to a kite mark.

Participants asked if entity categories were the same as certification marks. Certification marks require an audit, and although entity categories are auditable federations are not really working in this space at the moment. The InCommon R&S is self asserted, as is the Code of Conduct.

Andrew Cormack gave an overview of how certification marks are currently managed and their relationship to trademarks. There is an international organisation - WIPO, who might make this possible but it was felt that this would be incredibly complex.

Nicole Harris asked if there is added value in talking about certification marks, when we already have the term Entity Category. It is already accepted that Entity Categories can take many forms, including both auditing and self-asserted functions. Ken felt this was more about an audience problem in terms of phrases that could be comfortably understood by non-technical people, an issue of semantics vs syntax.

Overall participants did not feel that the certification mark proposal was worth pursuing and although it was recognized that it may be beneficial to use different language to explain our processes to end users caution was advised regarding the term 'certification mark' due to its current usage.

5. REF13-2: Baseline Assurance within Federations

Nicole Harris gave an overview of the current REFEDS plans to address immediate assurance issues for federations. This will focus on two areas:

- Establishing an agreed syntax for the R&S Entity Category value.
- Reviewing and proposing a common template for a Federation Operator Practice statement.

ACTION20130602-02: Nicole Harris to set up a call regarding the proposal for baseline assurance within federations.

6. REF13-3: requirements for eResearch

Licia Florio reported on progress on the REFEDS response to the FIM4R paper. A series of use cases have been received from the community, issued to both REFEDS and GEANT3+. These are currently being reviewed and a series of actions to work with the projects submitting the use cases will be established.

7. REF13-4: REEP Update

Leif Johansson gave an update on REEP, which is now available and live in pilot at reep.refeds.org.

The following actions are still to be completed:

- KMF establishment, key management and policy.
- Policy and operational practice statement.

Participants are advised not to add REEP metadata to production federations until the properly announced key management profile is in place.

If you have question about the service, please sign up for reep@refeds.org.

ACTION20130602-03: Licia Florio to send out details to REFEDS on how to join reep list.

Participants asked if any federations do more than domain validation for entities. For some federations this is the current baseline but there is a variety of practice that will feed in to the work on baseline assurance.

Participants asked about availability and reliability of REEP as a service and any SLAs around performance. REEP is currently on the Nordunet infrastructure as a PILOT only, but is a robust as we can get it without significant financial and time input.

REEP does not currently address or care about where certificates come from, so self-signed certificates will appear in the metadata. If an individual federation cares about this, it needs to strip off entities that it does't like from the REEP stream. It is not expected that any federation will necessarily be happy to consume REEP metadata wholesale.

Participants asked if entity category assertions will be included in REEP. It was agreed that REEP should support statements only if you are allowed to assert it yourself. Leif Johansson suggested that entities with certain tags should be published as an individual metadata stream, making it easy, for example, to grab an 'R&S' stream.

Participants asked if REEP should only be used be federation operators that know what they are doing. It was confirmed that REEP shouldn't be just used by end

entities at this point in time, but we are still exploring future models.

8. REF13-4: MET: Metadata Explorer Tool

Nicole Harris gave a brief update on the Metadata Explorer Tool, which intends to provide a simple graphical interface to statistics about entity data within federations. A call for MET2 has recently been issued and the results will be marked shortly.

Ian Young suggested that it would be useful for inter federation reporting if MET showed who had placed the metadata for entity x in edugain. This could be added to MET at a later date. Leif Johansson pointed out that web finger could be used for this.

This presentation closed the reporting on formal REFEDS work items. The afternoon session was devoted to new proposals and updates from NRENS and other projects

9. Shibboleth Consortium Update

Christoph Witzig gave an update on the Shibboleth Consortium and invited participants to consider joining.

10. New Proposal: Update on SCHAC

Licia Florio gave an update on SCHAC. The SCHAC schema was developed some time ago as part of the work of TF-EMC2 but has become a little stale. The schema is well used: edugain, TCS, perfsonar, and various federations rely on it. It is proposed that SCHAC should be migrated from TF-EMC2 to REFEDS, using REFEDS budget to help look after the schema. Will also be better supported by the REFEDS processes. Area where work is need includes:

- Tidying up the refeds website.
- Tool for access, do we need something better than a static html page?
- Address the call for the new namespace.
- Review vocabulary.

There is also an ongoing need to look at SCHAC versus eduperson, and another issue that has arisen recently is a home for an ORCID identifier as part of our schemas.

In order for this work to move forward, REFEDS will need a shepherd and owner for the work

ACTION20130602-04: Nicole Harris and Licia Florio to explore options for finding a SCHAC shepherd.

11. Federation as a Service

Federation as a service is a GEANT3+ work area looking at better supporting countries that do not have the capacity to set up their own federation. This will cover:

- SAML IdF and eduGAIN;
- eduroam;

- Moonshot.

Targeted groups are NRENS, institutions and large projects. The project is starting by exploring the issues that countries are facing whilst getting started (market analysis). The pilot will work with 10 selected NRENS to scope out an offering for Federation as a Service throughout the lifetime of the GEANT3+ project.

12. PERUN: User and Resource Management System

CESNET presented the PERUN tool – a similar service to Comanage. For CESNET the driver was a tool that would fill the gap between identity federation and services. PERUN has been developed for sometime at CESNET (since 1996). The background was management for national grid resources such as super computers. More information at: perun.metacentrum.cz.

PERUN is not currently available as a software release so only available as a service within CESNET.

13. SAML Test Harness Project

The SAML Test Harness Project is looking at tests that will challenge SAML infrastructure - eg. sending false certificates - to see if a secure infrastructure is in place. This work builds on fedlab – a GEANT 3 initiative. Testing needs to be on a community basis, looking at the overall testing of projects rather than being driven by one organisation alone. This test project encourages people to submit and show problems so that we can improve quality overall.

14. SUNET Update

SUNET are creating a common IdP for students in Sweden, accredited to Kantara AL2 with remote identity proofing and verification. This will be built to a very specific set of attributes as a complete solution for every use case. The intention is to bootstrap this service to local institutional identities and it will act as a proxy. This service is NOT intended to be an IdP to rule them all. SUNET are aiming for a state of the art credential management system.

The project will be actively developed on github: http://github.com/SUNET.

The full scope of what will be included (age, mobile number etc.) not set but the idea is that things that can be carried between schools will be in there. Identities won't be deleted so can always be used for any education transaction.

Participants asked what process would be used for identity proofing. There is a specific Swedish process in place that allows SUNET to do this, similar to the local paypal that knows most national IDs – with verification being carried out via low level transactions.

Leif Johansson also invited participants to look at the pyff metadata aggregator tool, full details of which can be found in the slides for this meeting.

15. Federation Operators Forum Proposal

Peter Schober proposed the establishment of a lightweight Federation Operators Group to run as part of REFEDS. This group would be closed and only open to current and potential staff directly involved in federation operations. The purpose of the group would be to allow discussion regarding technical issues that may be too sensitive for the main REFEDS mailing list.

Participants agreed that such a group should be established.

ACTION20130602-05: Nicole Harris to work with PS to set up mailing list for Federation Operators Group and provide support for meeting registration etc.

ACTION20130602-06: Peter Schober to propose some broad rules for operating the Federation Operators Group.

16. NSTIC Update

Ken Klingenstein gave a brief update on the work of NSTIC, including a piece of work that provided a comparison of 6 different (US) trust frameworks from NSTIC pilots: motor vehicle, SAML, Kantara, OIX. InCommon found to be the most robust. More information can be found at: https://spaces.internet2.edu/display/scalepriv/Scalable+Privacy.

Action Reference	Action Summary	Action Assignment
20130602-01	Discuss promotional materials with TERENA PR team.	Nicole Harris
20130602-02	Set up a call regarding the proposal for baseline assurance within federations.	Nicole Harris
20130602-03	Send out details to REFEDS on how to join REEP list.	Licia Florio
20130602-04	Explore options for finding a SCHAC shepherd.	Licia Florio and Nicole Harris
20130602-05	Set up mailing list for Federation Operators Group and provide support for meeting registration etc.	Nicole Harris
20130602-06	Propose some broad rules for operating the Federation Operators Group.	Peter Schober