REFEDS MINUTES, OCTOBER 2014

LICIA FLORIO AND NICOLE HARRIS

Abstract:
Miutes of the REFEDS meeting held 26th October 2014 in Indianapolis, USA.
Chairs: Nicole Harris (morning session) and Licia Florio (afternoon session)

TABLE OF CONTENTS

1. Review of REFEDS work - *Nicole Harris*

Nicole gave an overview of the achievements of REFEDS and on the ongoing work in 2014, which can be summarised as follows:

COORDINATION:

- the refeds.terena.org was recently migrated to confluence and is now wiki.refeds.org. There may be some broken links; the REFEDS groups is kindly asked to report any issues;
- blog.refeds.org could benefit from additional blog items, volunteers are welcome.
- plans are to revamp the refeds website at the beginning of 2015;
- REFEDS meetings: there are normally two meetings per year, which are co-located with major events, one of which being TNC. This year however, taking advantage of the European Identity Week (http://identityworkshop.eu/tiki-index.php) REFEDS will have another short meeting in Dec as well, focused on the plan for 2015.

WORK ITEMS:

- **Assurance** remains a difficult area. There is a need to establish what the 'baseline' common practises are for federations in this space today. REFEDS is working to create an unspecified REFEDS Assurance Profile that can be met by all existing federations. Initial work is online at: https://wiki.refeds.org/display/ASS/LOA+for+Research+and+Education+Federations. This baseline is driven by the FOP work (see below).

- Progresses have been made in the area of **Federation Operators Best Practice** (FOP). This work is defining Federation Operator Practice Guidelines which comprise of four documents, one of which available as draft. See https://wiki.refeds.org/pages/viewpage.action?pageId=1605961

- **Standards and specifications -** Main work in this area covers:
    - **SCHAC**, the schema for academia. The work is to harmonise the schema and deliver a consolidate version. This work is not funded with REFEDS budget. The goal is to move the management of SCHAC into REFEDS, once the schema is in order.
    - **Metadata Query Protocol -** to retrieve set of metadata. See the work in progress RFC: https://datatracker.ietf.org/doc/draft-young-md-query/.

- **Entity Category SAML Attribute Types -** how to form entity categories.
- **Entity Categories -** Two categories so far:
    - **Hide from Discovery,** approved rather fast,
    - as opposed to **R&S (Research and scholarship category)** that is undergoing a new round of consultation following the REFEDS meeting. LIGO is very interested in this category.

There is discussion on whether to start a new category **Library/affiliation,** which is rather controversial as an equal number of people think this to be needed/not needed. InAcademia the project funded by the GN3plus project could probably benefit from this category. InAcademia aims to build a inter-federation service to assert 'is this a student'.

- **Working groups**
  - The **FOG** (Federation Operators Group) is a closed group where admission requires endorsement from two existing members. All discussion on the list is confidential. However some of the discussion can be useful to derive best practices.
  - **MARI (managing attribute release in interfederation use-cases) -** Not a lot has happened. If nothing happens the group should be closed.

- **Pilots** - Two main pilots to date, MET and REEP. Work is planned to improve REEP UI.

Nicole also presented some preliminary ideas on the plans for 2015.

It was noted that it would be good to have a WG for CoC for nonEU/nonEU etc. within the 2015 work plan and work focused on the distributed resource registry work would benefit from a WG in REFEDS.

2. Coordinating International Efforts

EU initiatives, *Licia Florio*

Licia Florio gave an update on the work being carried out in Europe, and specifically the relation between AAI work within REFEDS, eduGAIN and the proposed AARC project. Attendees queried the best way to ensure that these groups are talking to each other and how to best influence the steering groups in each area. REFEDS is well positioned to take this role as the only independent and open entity.

Updates from ISOC, *Steve Olshansky*

Steve O gave an update on ISOC work in the space of identity and trust, including feedback on ISOC workshops (held in Sep 2014) looking at interfederation issues and attribute issues.

Updates on the US eGov work, *Ken Klingenstein*

Ken Klingenstein gave an update on NSTIC and FICAM developments. NSTIC looks at next generation services, privacy and so on. Currently is just US citizen to US Gov, but keen for it to be wider and more international.

Recently the US Gov announced the multifactor requirements for transaction from citizens to governments. The time frame is to allow for 90 days to specify the framework and 18 months to implement, also includes chip and pin.

Ken also mentioned that the US Government has recently joined InCommon.

Another area of work focuses on trust marks as opposed to trust frameworks and whether they need to be human readable, machine readable, or both. In NSTIC some of these are focused on machine-readable marks such as "does SAML2Int".

3. Assurance: Where are We?

SIRTFI group, *Dave Kelsey*

Dave Kelsey gave an update on the work of the SIRTFI group, which is focusing on the need for better definition of security incident response within the context of identity federations: https://wiki.refeds.org/display/GROUPS/SIRTFI. This builds on work discussed within the FIM4R group, REFEDS and as discussed at previous ACAMP meetings.

SIRTFI intends to build a lightweight framework that is self-asserted via an assurance attribute.

It was noted that we are often asked for these scaled-up approaches but then the SP in question will also happily use Google IDs that do not meet these standards. These inconsistencies need to be addressed.

Remote Vetting, *Valter Nordh*

Valter talked about the need to do remote vetting for students taking remotely courses and apply for a degree. The challenges is how to implement a simple system that at the same time preserve security and ensures the remote degrees are given to the legit people. Many of the traditional models (credit card transactions, utility bills etc.) do not work for students. One possible solution might be mobile money.

Work needs to be done on understanding what the SP actually requires versus what they ask for. Vetting at student registration may be less important than giving assurances that the same person is returning.

IETF Vector of Trust, *Leif Johansson*

Leif presented the ideas behind the Vector of Trust. During the ISOC meeting in Sep 2014 they tried to identify and set of vectors and baselines requirements to build a lightweight trust framework for identity assurance. Four vectors were identified:

- ID Proofing
- Credential strength
- Assertion presentation
- ops management

For each of them they identified some characteristics that do not necessarily map existing frameworks. Further they looked at the syntax. The resulting work would be used as the building block for existing and future trust frameworks. The hope is that

existing framework would have to reference to this underlying framework.
The gain of using this would be making comparisons easier, to have a common syntax and to allow IdPs to implement only one of aspects of LoA rather than a whole framework.

Many federations spend significant resources to onboard services; Leif noted this process could be improved by outsourcing the process for instance, which could become a (global) service. The vot@ietf.org list is for discussion of a common set of baseline "vectors of trust".

4. Supporting Virtual Organisations

Enabling group management in eduGAIN using PERUN system, Michal Prochazka

Michael gave an overview on PERUN, the tool to manage virtual organisations groups. The tool also does credentials linking (SAML, X.509 and social) and supports VOOT. The presentation focused on PERUN's usage in eduGAIN. Michael noted the tool appears in the discovery service but they should not.

Attribute and group providers - What's out there?, Maarten Kremers

Maarten reported on the work done to compare the various attribute management systems. The aim if to produce a white paper at the end of 2014. Maarten asked everybody for feedback. See the comparison at: www.bit.ly/aa-overview.

LIGO updates, Scott Koranda

LIGO are keen to use federated access approaches but attribute release is the single most important problem in moving this forward. LIGO seriously need to see R&S implemented by federations to enable them to use our infrastructure. Scott noted that they would really need to see eduPersonPrincipleName populated. There is a call to all federations to move forward in this space.

5. Schemas, Specifications and Standards Update

SCHAC updates, *Heather Flanagan*

SCHAC has languished for a long time and lots of things need fixing. Heather has been appointed to help tidy up the issues. Major problems including fixing things that are specifically wrong, fixing deprecated documentation and putting in place a new governance model.

REFEDS RFC work, *Heather Flanagan*

REFEDS is using the Independent Submission Stream to submit documents for publication in the RFC Series.

One document has been submitted through the REFEDS independent stream:

“The Entity Category SAML Attribute Types” <draft-young-entity-category-02>. The ISE is going above and beyond his usual efforts to make sure this draft (and the REFEDS ‘boilerplate’) gets as much exposure as possible

If REFEDS ever wants a document to be more than just an Informational RFC, we need to request a working group within the IETF. Members of the IESG would like that very much.

Next documents to be submitted are:

- Metadata Query Protocol - <draft-young-md-query>;
- SAML Profile for the Metadata Query Protocol - <draft-young-md-query-saml>.

Entity Categories, *Nicole Harris*

There are two entity categories out at the moment open for feedback. After the consultation period expires they will be published on REFEDS (not via the IETF-RFC).

Hide from Discovery: a list of IdPs that do not want to be in the discovery. Some minor changes mostly relating to the language.

The R&E category required more work. The initial motivation to review the category was to fix an error in one of sentences. Further more comments were submitted but the main topic of discussion was to agree on the definition of the R&E category.

There might be a new category about affiliation. The discussion on whether to continue with this work has been inconclusive. This category could be useful for inAcademia [1]; a service that aims to enable discounted services for the R&E community.
Leif noted that the inAcademia would be really appreciate the EntCat.

Monitoring Tools Update - *Roland Hedberg*

Roland presented the list of tools he developed to validate the federation metadata to ensure they work properly. The tools look very promising:

- Saml2test - checks implementation/installation conforms to the standard and the profile
- Metadata analysis - e.g. http://monitor.edugain.org/coco
- Verify_entcat - verifies that an IdP is compliant with an entity category
- metadata consumption check service - checks if an IdP wants to talk to an SP
- IdP monitor - verifies the whole authN process works for a user.

See https://github.com/rohe

6. Impact of Interfederation

Overview, *Nicole Harris*

Nicole gave an overview on the main inter-federation issues at the moment. See more at blog.refeds.org.

Update from UK, *Rhys Smith*

Rhys noted that as Nov UK will move from opt-in to opt-out. No entity in the UK is tagged with entity category yet. Rhys noted that the only way for eduGAIN to be successful is convince federations to adopt opt-out, to have one stream of metadata. Currently UK represents just 7% of eduGAIN. By the end of the year apart from schools and some specific test IdPs or wildcard IdPs all of the UK metadata will be in eduGAIN and will make up 70% of eduGAIN.

Update from US, *John Krinke*

John gave an update on the issues that InCommon faced joining eduGAIN. Three main issues are listed below:

- InCommon Participation agreement in 2004 never had indemnification in it. In discussions with lawyers about eduGAIN concerns have been raised about indemnity.
- The original agreement only mentioned publishing metadata to *InCommon* participants. To be able to share their metadata with eduGAIN a change is needed to the Participation Agreement.
- US Import laws are pretty liberal, but exporting metadata has PII (i.e. contact details) so they are checking the legal implication of this - although practically it is public information so shouldn't be an issue.