REFEDS Minutes, 22 April 2012

Licia Florio and Nicole Harris

Abstract:

Minutes of the REFEDS BOF held in conjunction with the Internet 2 Spring Member Meeting. For more information see: https://refeds.org/meetings/apr12/index.html.

Table of Contents

1. Introduction

Nicole welcomed everyone to the meeting and asked attendees to introduce themselves. Throughout the day, there were on average 40 people in attendance at the meeting. Nicole explained that as this was a BOF we would not be covering the entire set of REFEDS workpackages, but would look more deeply as some of the areas of specific interest to attendees. bfrr

2. PEER – Leif Johansson

The PEER project was mostly funded thanks to ISOC contribution. PEER is intended for low assurance services that need to have their metadata consumed in various locations – examples would be the REFEDS and Shibboleth wikis.. YACO have now delivered the PEER code and are on a 1 year maintenance and bug fix contract.

REFEDS now needs to consider a governance and service model for a public research and education PEER service.

Attendees were asked to consider the conditions on which they would make use of PEER: personal data exchange, metadata format and management of keys were both mentioned as important areas to address.

Metadata Exchange

Federation metadata currently looks and behaves very differently, depending on the local requirements of federations. A PEER pilot should help us understand how many problems and issues these differences would cause. Ian Young described the UK federation process of striping metadata to make it consumable within the UK production aggregate. It is likely that use of PEER will create a need for more complex metadata management at the local level. REFEDS and PEER will need to establish a set of first principles for metadata to be included in PEER that can be accepted as is by federations. This should refer back to common standards models.

It was further acknowledged that there is still a long way to go to help people understand the different between signing a policy and registering technical data. Separating the flow of metadata from the flow of trust is a new concept for most federations.

PEER and eduGAIN

A common question we must be ready to answer is, what is the difference between PEER and eduGain? They are effectively very different in that eduGain is an aggregator of metadata, PEER is a metadata registry. Ian Young created a useful paper to explain this concept, available from his blog.[1] In the PEER model, all you have to do is prove that you own a domain, and this then allows you to register entities against that domain. The main use-case for PEER seems to be the centralised place to distribute metadata to facilitate its consumption and the separation between the flow of metadata and the flow of trust. In the long-term it may be possible for eduGain to take feeds from PEER.

Neither PEER nor eduGain currently have any specific recommendations at a level of metadata entity construction. What should a PEER service be looking to standardize on?

ACTION20120422-01: Licia Florio and Nicole Harris to look at PR material for PEER, including specific use cases for the service.

ACTION20120422-02: Licia Florio to contact REFEDS-SC and appoint a working group to prepare governance and service structure for PEER to present at TNC2012. Aiming for a pilot to start in the summer for a 1y period.

3. Attributes Release Working Group - Mikael Linden and Steven Carmody

Mikael summarised the directives that led to the creation of eduGain / GEANT Code of Conduct, to simplify the release of attributes when parties inter-operate. The drivers for the Code of

[1] Concepts and Methods: http://www.iay.org.uk/blog/2009/05/concepts_and_me.html.

Conduct were to enable cooperation to reduce the risks close to a point that is acceptable to parties and does not require contracts.

The Code of Conduct will be trailed in EU, as the EU has the strictest data protection framework in place. The name derives from suggestions in the EU directive on data protection. It is worth stressing that SP need to declare they follow the code of conduct, it's a unilateral declaration! Contracts are not signed between the declaring party and a central body.

One approach for release is consent: if IdP uses consent to release attributes to SPs, SPs would have to be satisfied that consent was properly obtained (complex!); this approach was not followed. The approach followed instead is that SP commits to meeting requirements under the Code of Conduct; the SP makes a public statement (unilateral declaration) that the will behave legally. The IdP may decide to inform the users on the attributes that are being realised.

Some issues have been identified with expanding this model to non-EU countries (the EU law seems to require signatures for this).

The WG will carry out the work until version 1.0 of document is out - this is expected to happen in the summer 2012. The current version of the Code of Conduct is available at: https://refeds.terena.org/index.php/Code_of_Conduct_for_Service_Providers.

ACTION20120422-03: Steven Carmody to send an update from the Attribute Release working group to the list.

4. Discovery and MDUI – Rod Widdowson

Rod gave an overview on the current status and use of MDUI within federations. Attendees noted it would be of great value if REFEDS (Rod) could come up with a set of light weighted recommendations on how to implement MDUI

Rod asked how federations implement MDUI:

- **InCommon:** started to ask display name for SPs, long term to ask that for IdP;
- **SWITCH-AAI**: manually prefill info for the IdPs, which can correct the info. Description is left open (or the long name is used); the length of the field may be a problem when this field is displayed, although not artificial short-name should be used, better to use a ... in the middle for instance. Also includes IPHint, DomainHint and GeoLocation where possible;
- **UKFed**:ask for logos, displayname and description.Happy to populate all fields if requested;
- Japan: implementing MDUI, they are using SWITCH tools. This includes logo, DisplayName, Description and Hints.
- SURFnet is populating MDUI for surfConnext.

Has REFEDS reached the point to push federations to use some common practice in these areas? Rod and the attendees felt that after consensus is reached REFEDS could do that and this would naturally lead to recommendations on the MDUI.

Problem areas:

- It was noted that dealing with logos is a rather tricky process: what should be the default logo in the absence of a logo?

- Long names and limits around the number of characters is an issue. Can software help collapse with (ccc….cccc). Is shortening in the middle an option here?
- Language tags are useful, but browser settings more often relied upon.

ACTION20120422-04: Rod Widdowson to draft a set of best practices for MDUI and present them at TNC2012.

5. Specification updates – Leif Johansson

Leif gave a broad update on several activities with the standards space that are relevant to identity federations.

Entity Categories

Macedir.org

Leif described the concept of Entity Category Attributes: the idea that you can generally say that this entity is of type X. A specification for this has been developed and is available at macedir.org. Generally this is to allow us to assign entities to groups such as 'research', 'student service' etc so IdPs can better understand the purpose of the SP and potentially be more confident in releasing attributes and engaging with this service. This approach is purely a way of describing the entity attribute – it is not a registry, nor does it provide profiles for this at the moment. There is no hierarchy in the process, and can be multi-valued.

Attendees asked if any work been done to work on a higher education profile for using entity categories? At the moment, no but InCommon has started developing these. We hope that these will be shared to achieve common practice across federations.

ACTION20120422-05: ALL look at the entity category specification and comment.

MDX spec –

Leif and Chad have put up a current draft for a metadata exchange (mdx) specification on github: https://github.com/lajoie/md-query. This is the start of a process to establish the specification for metadata exchange. Please join the list and comment at: mdx@lists.iay.org.uk . Join at: http://lists.iay.org.uk/listinfo.cgi.

ACTION20120422-06: ALL read the metadata exchange specification and comment.

LoA registry –

LoA are generally associated with trust framework, but there are potentially many frameworks in use, i.e. Kantara, I2, FICAM etc. Leif has written an IETF draft (draft-johansson-loa-registry) as an individual publication. There needs to be an effective way of describing the assurance profile being used within an entity description. There is already a way of tagging this via an entity attribute, but there is no common way of expressing the framework this entity tag describes. Is this a NIST descriptor, a Kantara descriptor or an InCommon descriptor and how are they linked?

The proposal suggests an IANA registry for Level of Assurance Profiles. There are current issues with the best way to manage publication of such a profile, particularly when considering the IETF process.

ACTION201204220-06: Licia Florio and Nicole Harris to explore the IPR requirements for IETF specifications and discuss this as a sensible model for developing and publishing work within the REFEDS context.

Attribute Registry

There seems to be interest in having registries for attribute definition. The problem of how to represent attributes beyond x.500 is gaining significant interest. This would be a complex space reaching beyond the boundaries of REFEDS (e.g. SCIM), but seems worthy of exploration and involvement, What would the set of requirements be if you wanted to create an attribute registry? Leif has started a discussion on this within IETF and will report further as work develops.

DiscoJuice and Account Chooser

Google have been working on a specification for AccountChooser, which allows a user to more effectively manage their identities in a process similar to the DiscoJuice or Shibboleth EDS work. AccountChooser have decided that they will not be hosting this themselves. There is an opportunity here for REFEDS to engage this with their work through the Discovery Project. The bigger question here is what discovery looks like when you combine OpenIDConnect and SAML metadata. A current question is whether we should common domains for discovery or not - a similar discussion to central vs. embedded discovery.

ACTION20120422-07: Nicole Harris, Leif Johansson and Rod Widdowson to engage with WH @OIDF to make account chooser work in the federation space, possibly as an extension to the Discovery Project.

LEGO Updates

The initial work in LEGO has been completed merely as an exercise. A couple of federations have looked at mapping OIX FICAM LoA1 to their current federation policies. There are a few areas that may cause current problems to federations: insurance requirements and specific jurisdictional requirements. It would be helpful if more federations could map their current practises against this process. Gakunin have been through an accreditation on OIX – it would be good to capture this information.

ACTION20120422-07: Call for other federations to undertake a mapping exercise as part of LEGO for FICAM, Kantara and OIX frameworks.
ACTION20120422-08: Gakunin to report on their OIX accreditation process to the REFEDS list.

6. Trust Framework – Kazu Yamaji

Kazu described recent developments in extending the trust framework for Gakunin. The main motivation to connect to NIH (national Institution of Health) services and to apply for grants for Japanese authorities (e-RAD). Gakunin explored 2 options: an agreement between NII and NIH and the OIX process.
Areas that needed work:

- Reorganization of the way Gakunin team works.
- Maturity of institutions.
- Fees.
-

Gakunin are also working with OpenIDConnect to look at the possibility of acting as an Attribute Provider to OpenIDConnect. This raises questions over the authority of a 'student' attribute release.

7. Inter-federation and metadata management - Ken Klingenstein

Monetisation of attributes is growing (see Google verifying email addresses by verifying the postal address of the individuals). Can REFEDS do something about this?

8. Action Summary

- **ACTION20120422-01**: Licia Florio and Nicole Harris to look at PR material for PEER, including specific use cases for the service.
- **ACTION20120422-02**: Licia Florio to contact REFEDS-SC and appoint a working group to prepare governance and service structure for PEER to present at TNC2012. Aiming for a pilot to start in the summer for a 1y period.
- **ACTION20120422-03**: Steven Carmody to send an update from the Attribute Release working group to the list.
- **ACTION20120422-04**: Rod Widdowson to draft a set of best practices for MDUI and present them at TNC2012.
- **ACTION20120422-05**: ALL look at the entity category specification and comment.
- **ACTION20120422-06:** ALL read the metadata exchange specification and comment.
- **ACTION20120422-07**: Nicole Harris, Leif Johansson and Rod Widdowson to engage with WH @OIDF to make account chooser work in the federation space, possibly as an extension to the Discovery Project.
- **ACTION20120422-07**: Call for other federations to undertake a mapping exercise as part of LEGO for FICAM, Kantara and OIX frameworks.
- **ACTION20120422-08**: Gakunin to report on their OIX accreditation process to the REFEDS list.
-
-