REFEDS Planning: 2013

- REF13-1: REFEDS Coordination and Management
- REF13-2: Defining baseline assurance within federations
  - 13-2a: Federation Operator Best Practice Documents
  - 13-2b:Data protection Code of Conduct -- extending beyond the EU/EEA
  - 13-2c: Levels of Assurance: What's My Level?
  - 13-2d: Entity Categories.
- REF13-3: Engaging with eResearch
- REF13-4: Understanding and improving metadata flow across federations
  - REEP
  - MET / Service Provider Status Tool
  - Scaling of (inter)federation
- REF13-5: Specialist Work Areas
- Parked Items
  - IdP of Last Resort
  - Single Logout
  - The Role of the Attribute Authority / Provider

REF13-1: REFEDS Coordination and Management

This area to include maintaining the website, kick starting the blog, finishing the RFC work, REFEDS promotion and administration.

Lead: Licia Florio / Nicole Harris

Aim:

- To progress REFEDS position as an important player within the access and identity management space internationally.

Work Items:

- Establish better understanding of workflow between tf-emc2, GEANT and REFEDS.
- Continue developing relationships with Kantara, ISOC, NIST and NSTIC.
- Continue evolving REFEDS communications channels.
- Develop working with MET to inform REFEDS intelligence.
- Establish contact point for queries from REFEDS outputs (discovery project work, PEER / REEP contact point).
- General admin for meetings, mailing lists and supporting infrastructure.
- Complete work on RFC.

Sponsored Output:

- 2 x REFEDS BOFs with specific community focus.
- www.refeds.org maintenance/development.
- Maintaining the REFEDS blog.
- 2 x standard REFEDS meetings.
- REFEDS PR material (newsletters, REFEDS map).

Time Allocation:

34 days REFEDS coordinator time over the period 1 January 2013 – 31st December 2013.

Budget:

€30,000 – including travel costs.

REF13-2: Defining baseline assurance within federations

REF13-2: Defining baseline assurance within federations

Lead: Nicole Harris

Aim:

- To improve the understanding of the base assurance of federations and to improve the usage of federation infrastructure based on increased assurance understanding and implementation.

Work Items:

- Develop a federation operator best practice template in line with the federation policy template (13-2a).
- Further develop the 'Code of Conduct' to be applicable for international attribute exchange (13-2b).
- Develop a plain English mapping tool for federation assurance across common assurance profiles and make recommendations for an R&E assurance profile based on this work (13-2c).

Sponsored Output:

- FOP Template.
- Assurance mapping tool.
- Recommendations for R&E assurance profile.
- International Code of Conduct.

Time Allocation:

Up to 40 days of coordinator / editor effort across all the three work areas. Budget:

Up to €30,000. This does not included fees for lawyers for Code of Conduct work (for discussion with GEANT).

13-2a: Federation Operator Best Practice Documents

Proposed by: Brook Schofield / Leif Johansson.
Concept: Create a template best practice document looking at federation operator practices with a technical focus, to compliment the work on policy that has been carried out in 2011/12. Note that InCommon, and perhaps other federations, already have a fairly detailed practices document that might be useful here.

Resources Needed: Would need around 15 - 20 days effort from an editor
Timescales:
Support: +12 (Feide, Heather Flanagan, Peter Schober, Mikael Linden, Lalla Mantovani, AAF, Edugate, Andrew Cormack, David Simonsen, Valter Nordh, Ken Klingenstein, AAI@EduHr(Miro))

Notes from REFEDS 2012

Initial idea came out of tf-emc2 with mostly a focus on aggregation. An operator template would be much wider than this focus.

In order to achieve interfederation, we spend a lot of time a) assuming what the other federation is doing and b) assuming it is 'the right thing'.

What do want to see in the template. Is this simply a list of check boxes? Is this a more detailed piece of information? Check boxes would allow us to machine check this at some level.

What would some of the questions be?

- Membership application processing;
- Registration of entities;
- CA qualification;
- Monitoring;
- Do you perform checks on what attributes are being asked for by Service Providers and why they are actually being requested?
- Error handling? (probably not)
- What does 'the metadata is correct' mean? Saml2int?

Milan raised the issue of these type of discussions around PKI looking at this type of thing and not getting very far.

If GEANT takes forward the idea of a FOP template for new federations we will need to try and join up with this work.

Leif noted that we should align with the KANTARA Federation Operator Guidelines (or something like that).

13-2b:Data protection Code of Conduct -- extending beyond the EU/EEA

Proposed by: Mikael Linden, Steven Carmody
Concept: The Data protection Code of Conduct describes an approach whereby both Home Organisations and Service Providers can acquire confidence that the other party is meeting its data protection requirements under the EU Data Protection Directive; it was developed last year and has been through a comment period. This new effort would extend the CoC framework to cover attribute release to countries outside the EU/EEA area. This work would be conducted together with GN3/GN3+ project. It would also be used by the InCommon NSTIC work to inform, if not affect, US policies.
Resources Needed: Lawyer to design the legal framework (GN3 has used DLA Piper).
Timescales: Starting 4/2013 (GN3+ starts)
Support: +8 (Heather Flanagan, Lalla Mantovani, RENATER, SURFnet, Peter Schober, Valter Nordh, Ken Klingenstein)

13-2c: Levels of Assurance: What's My Level?

Proposed by: Leif Johansson, Nicole Harris
Concept: Many federations already implement rules or require terms of use that provide a base level of assurance for IdPs, but it is often difficult to understand how these relate to different assurance profiles (Kantara, FICAM etc.) REFEDS should create a tool that allows people to map their current practises and processes to assurance profiles - for example "We do not allow plain text passwords to be transmitted" maps to AL1_CO_SCO#020 in the Kantara Identity Assurance Framework Service Assessment Criteria. Note that it would be nice to come up with an international R&E "Silver" equivalent as well as doing a comparison tool
Resources Needed: 2 days per framework for analysis (up to 5), 2 days to define assurance areas, up to €5,000 for development of a mapping tool. Up to 5 days work on recommendations and presentation.
Timescales: Work to be completed by December 2013.Recommended that work should start after FOP template is created to help inform.
Support: +13 (Feide, Heather Flanagan, Peter Schober, Mikael Linden, Lalla Mantovani, RENATER, SURFnet, Ajay Daryanani, Ann West, Valter Nordh, Ken Klingenstein, AAI@EduHr(Miro), Jim Basney)

13-2d: Entity Categories.

Summary of attribute release requirements from REFEDS mailing list discussion.

REF13-3: Engaging with eResearch

Lead: Licia Florio

Aim:

- To work on the recommendations put forward by the FIM paper. This work item will identify specific topics and will offer proposals on how they could be addressed by the Identity Federations community, eduGAIN and the related e-Research communities.
- To offer an international forum where specific e-Research use-cases (i.e., LIGO) can be brought forward and discussed.
- To discuss how better leverage existing (inter)federation infrastructures
- This work will also consider the work planned by the “Attributes In Motion Work Group” operating within Kantara.

Work Items:

- The specific work items will be listed in the paper (which is expected by end of Nov). Possible work items include, support for LoAs in existing federations, recommendations on attribute providers etc., Working group addressing the role of Attribute Authority / Provider within federations.

Sponsored Output:

- Recommendations on how federations should address the role of Attribute Authority (Provider).

Time Allocation:

- 30 days.

Budget:

None requested at this moment, however budget may be needed if it is agreed to carry on specific work as result of the “Roadmap to address FIM4R Requirements - FINAL Version ”.

'**Resources**'

- First FIM4R workshop, held at CERN in June 2011.
- Second FIM4R, at RAL in November 2011 .
- Third FIM4R, at ISGC in February 2012.
- Fourth FIM4R, in Nymegen.
- Fifth FIM4R, in Villigen .
- FIM4R paper for which comments are welcome.

- FIM4R Use Case Gathering.

REF13-4: Understanding and improving metadata flow across federations

Aim:

- To increase the exchange of metadata across federations and to improve the understanding of interfederation practises and process amongst federation members.

Work Items:

- Run a pilot REEP service for the research and education community for 2013, making recommendations for a future service environment.
- Develop MET to provide clear information on Service Provider status, which federations they are part of and where metadata is being consumed by federations participating in interfederation agreements.
- Address the concerns of scaling for federations.

Sponsored Output:

- Recommendations from REEP pilot to the community.
- REEP website and pilot service.
- Enhanced MET interface in use with federations, IdPs and SPs.
- Report on federation scaling.

Time Allocation:

- 20 days coordinator work for REEP and MET.

Budget:

€10,000 for coordinator support and expenses, €5000 for infrastructure support and software installation.

REEP

This work area will move REEP forward in to a one year pilot project hosted at Nordunet.

- Proposed workplan for 2013
- REEP Overview 2013
- REEP Policy

Action items:

- REEP integration guide. How do I get information out of REEP and in to my federation? Aimed at federations (NH)
- Promotional material for Service Providers. (NH)
- Getting the MDX spec completed within the IETF space. (IAY)
- Bug-fix and maintenance contract with Yaco.
- Installation costs and New Features (Yaco).
- Website costs.
- A richer set of policies between aggregators.
- Complete the PEER FAQ.
- Complete the set-up of the REEP mailing list.
- Sustainability plan.
- Complete policy and publish.
- PEER the software: Use the existing list for the technical discussion on PEER features and advertise that.
- Create a team to look at the REEP service definition for the pilot and describe what happens if REEP doesn't continue and if REEP is migrated to another place. The trust model for REEP should also be addressed.

MET / Service Provider Status Tool

Proposed by: Nicole Harris / Brook Schofield
Concept: Using the MET tool, create a promotional tool / website that can be used to show which federations SPs are currently members of, where their metadata is available, what interfederation arrangements SPs are available through, where interfed metadata is being consumed, and to allow federations to express interest in SPs joining / providing metadata.
Resources Needed: Would imagine working with Yaco / TERENA staff on how to implemen, possibly external support from designer?
Timescales: Jan - Jul 2013
Support: +6 (Feide, Heather Flanagan, Lalla Mantovani, AAF, RENATER, AAI@EduHr(Miro))

Feedback on MET

Scaling of (inter)federation

Proposed by: Mads Freek Petersen, David Simonsen, Michael Gettes
Concept: Imagine how hundreds of thousands of federated entities should be handled. It seems obvious that today's federations can't do the job. The task is to suggest a workable solution to the two related problems:

- handling of large numbers of federated entities
- handling of trust in large federations (whatever that means in this context)

A break-out session on the matter was held during the Advanced CAMP in Philadelphia, fall 2012, minutes can be found at: https://spaces.internet2.edu/display/ACAMPScribe2012/Fri+8.45am+Salon5
Resources Needed:
Timescales:

Support: +11 (Feide, Heather Flanagan, AAF, Andrew Cormack, RENATER, Niels van Dijk, Chris Phillips-CAF, Roland Hedberg, Ken Klingenstein, AAI@EduHr(Miro), Jim Basney)

REF13-5: Specialist Work Areas

Lead: Groups lead by proposer as appropriate

Aim:

- To provide infrastructure and support for evolving ideas and areas in the REFEDS community.

Work Items:

- Write to proposers of working groups explaining expectations and facilities for groups within REFEDS.

Sponsored Output:

- None.

FOG: Federation Operators Group

FOG

STORK / SAML Interop

Notes from the first Interop Call

Parked Items

IdP of Last Resort

Proposed by: Chris Philips
Concept: Formally define 3 types of IdP Appliances that could be deployed either in a public cloud or private cloud 'at scale':

- Standard IdP that connects to a directory/DB
- an IdP that connects to a directory/DB and also offers self sign up facilities
- an IdP that behaves as a gateway for SOCIAL identity protocols to SAML

Resources Needed: 1.5 FTE, 2 months full time and attention? (big guess & depends on environmental scan)
Timescales:

- By no later than Nov30 2012:
  - Environmental scan and attempt at cataloguing existing efforts & offerings
  - capture business & technical requirements
  - craft a written report recommending a path to follow for builds, support etc of appliance model
- By no later than March 1, 2013
  - Initial pilot of at least one of the appliances depending on outcomes of environmental previous steps
  - Operationalizing the approach and identify the gaps.

Support: +2 (SURFnet, CAF(ChrisP is part of))

Single Logout

Proposed by: Chris Philips
Concept: Review the current state of Singe Log Out approaches for SAML, evaluating the risks & benefits of possible enhancements and investments such that end users and IdP operators benefit.
Resources Needed: Quantity of work estimated as 2 FTE 1 month full time and attention which would include dev work based on recommendations. Actual work would occur over a longer time period
Timescales: Timescale is hard to estimate as there is no hard driver other than improving user experience & mitigate risk by poor browser behaviour

- Definition & Scoping Phase:
  - capture business & technical requirements
  - Perform environmental scan, attempt cataloguing existing efforts & offerings with assessment of shortcomings and possible improvements
  - craft a written report recommending a path to pursue for improvements along with guidance on patterns, techniques and limitations.
- Proof of concept Phase:
  - based on report from first phase, define statement of work and confirmation of effort to implement

    - provided SOW is accepted, implement and allow the community to test implementation and provide feedback
    - based on feedback perform alteration and define a major x.0 release
- Encourage Broader adoption Phase:
    - supported by adoption of techniques and approaches, identify recommendations to be offered to OASIS to enhance the SAML profiles

Support: +5 (Feide, AAF, Edugate, CAF(work proposed by ChrisP), AAI@EduHr(Miro))

The Role of the Attribute Authority / Provider

Proposed by: Niels Van Dijk
Concept: From previous discussions, in the REFEDs list, as well as e.g. at the Utrecht VAMP meeting, it seems clear that Attribute Providers (AP) may come to play a much more important role in the near future.
Scenarios where these may come in handy include: 'Bring-Your-Own-Identity' where e.g. students bring in a social ID, which then gets decorated with campus attributes, a VO who takes the IdP authN, but adds VO attributes on top of that.

Much of this is 'undiscovered county', popping up questions like:

- what are the common scenarios for working with APs,
- is there a common vocabulary when working with APs,
- how do we register attribute providers? (best practice available?)
- how is trust established for APs, the same as for SPs, or IdPs or different?
- will we need a 'AP code of conduct'?
- should an AP be a member of the Federation?
- does the concept of an AP at all exist in your federation policy?
- do we only allow/need SAML based attribute providers, or also e.g. OAuth/JSON based ones?
- how and in what way does REFEDs liase with other projecst that work in this area
- what are the transports, and associated protocols and issues, for moving attributes from an AP to an IdP. Note that this is a part of the InCommon NSTIC deliverables.

Resources Needed:
Timescales: 1 year +
Support: +6 (Andrew Cormack, Roland Hedberg, Valter Nordh, Lalla Mantovani, Ken Klingenstein, AAI@EduHr(Miro))

Notes from REFEDS Nov2012

Ken raised some of the issues described in gpii.net/index.html and the ideas around: https://spaces.internet2.edu/display/scalepriv.

Proposals from the floor:

(NH) we need to be very careful about the vocabulary we are using and how we use it. Attribute Authority has a very specific meaning in Shibboleth, and there is currently no shared understanding of what we mean by Attribute Provider.

Action: Ken to circulate his plan to the REFEDS list and to ask for volunteers. Ken proposed Steeve O to chair the group.

Action: Move the attribute providers work to workpackage 5.