2015 Work Plan Preparation

Please use this page to record ideas that you would like to include in the 2015 workplan. Copy and paste the table below. Ideas don't need to be fully formed but the more scope we can get the easier it will be to assess whether idea should be taken forward. We look forward to all your ideas!

updated 17th December 2014 Many thanks for all of the inputs - this will now be combined with ongoing work items and discussed by the REFEDS SC. A formal word document will be shared in January 2015.

- Template
- Ideas
  - Group 1: Global services: incident response, helpdesk and central monitoring tools
    - Fed Ops Security Incident Response
    - Global FedLab
    - EduGAIN Global incident handling/support framework
    - Federated Error Handling
  - Group 2: Virtual Organisations and Groups
    - VO Assessment
    - Focus on VOs
    - Attribute authorities and group membership/role information
  - Group 3: Federation Operator Best Practices
    - eduGAIN Recommended Practices
    - Focus on R&S adoption
    - Contacts in Metadata
  - Group 4: Alternative Methods of Metadata Distribution and Discovery
    - Federation at scale
    - Fresh Approaches to IdP Discovery
  - Group 5: New Working Groups
    - Privacy and interfed
    - Best practices for Hub-and-Spoke federation

Template

Title	**<title of your proposal here>**
Description	<description text here>
Proposer	<your name here>
Resource requirements	<money? effort? coordination? unicorns?>
+1's	<for others to voice their support - add your name here>

Ideas

Group 1: Global services: incident response, helpdesk and central monitoring tools

Title	**Fed Ops Security Incident Response**
Description	Most federations have wording in their federation policy to support incident response but this tends to be a few words committing the Op, IdP and SP to work together on issues. There is no developed idea of the workflow for incident reporting and it is difficult for SPs to understand the process across different federations or contact multiple federations. REFEDS should define a common process and workflow descriptions for federations and support a lightweight model for supporting incident reporting and discussion - possibly via the FOG list or an XMPP type approach. As discussed at ACAMP.
Proposer	Nicole on behalf of ACAMP session.

Resource requirements	REFEDS Coordinator time, buy in from federations, possibly some small infrastructure support requirements.
+1's	Tom Barton, Wendy Petersen (CAF), Dave Kelsey, Scott Koranda, Romain Wartel, Michal Prochazka, Ann West, Heather Flanagan, Lukas Hämmerle, Jean-François Guezou
Consensus	Proceed - keep lightweight.

Title	**Global FedLab**
Description	Lots of useful tools have been produced as part of FedLab - as seen in Roland's excellent presentation in Indianapolis. There have also been other tools developed across the community to monitor and check information - such as MET, Code of Conduct monitor, Lukas's domain-checking tool for edugain, SMEV etc. etc. Some of FedLab will be moved to production as part of the GN4 project under the Identity and Harmonisation Task, but this will only address specific GEANT Project use cases. A pilot should be undertaken by REFEDS to look at global requirements and the best set of tools for our community. In the longterm this may merge back with GEANT service offerings but it makes sense to run a pilot under REFEDS to address all possible features.
Proposer	Licia Florio, Nicole Harris, Roland Hedberg
Resource requirements	Funding for hosting and coordinating testing and decisions around useful tools. Development effort can be provided via GN4.
+1's	Tom Barton
Consensus	Proceed

Title	**EduGAIN Global incident handling/support framework**
Description	As national federations continue to join eduGAIN the problem of supporting users across federation boundaries will increase. When a user has an issue attempting to access services provided in another federation how it will be resolved in this global federation of federations. Issues the end user may experience include; • Understanding where the cause of the problem is; • Language barriers; • Service providers unaware that their services is available in other federations; • Services providers unwilling to provide support to users in other federations; • Global scale and time zone difference challenges The development of a global incident handling/support framework. This framework would build on each federation's user support strategies and seek ongoing support of the framework from federation through a memorandum of understanding.
Proposer	Terry Smith (AAF) and Sat Mandri (Tuakiri)
Resource requirements	1) Development of a service oriented approach eduGAIN Global Support Framework to provide seamless user experience, including: i. Capability to log support request from anywhere (eduGAIN Support Zendesk) ii. Incident Management process for National Federation on eduGAIN iii. Incident Management process for Service Providers (Institutional, National, and International SPs) 2) A program of work to ingest (1) above into all national federations participating in eduGAIN. Development and documentation of the framework Marketing of the framework and buy in for federations
Risk and Issues	eduGAIN to publish a register for participating members to log and manage Risk and Issues
+1's	Heath Marks (AAF), Wendy Petersen (CAF)
Consensus	This is an edugain operational issue and some of the info is being looked at - e.g. helpdesk functionality in GN4. Not for REFEDS.

Title	**Federated Error Handling**

Description	Develop a systematic approach to error handling at the Service Provider, especially in the common case where there are no (or too few) user attributes in the SAML response. One approach that has been suggested (but is by no means the only approach) is to leverage the Error Handling URL (`errorURL`) in IdP metadata so that end users are directed to an appropriate service point (e.g., help desk, IdM support, etc.). A possible outcome of this work item might be a simple profile of the `errorURL` in IdP metadata and a strategy for increasing its usage worldwide.
Proposer	Tom Scavo
Resource requirements	Profiling the use of `errorURL` in IdP metadata (if that is indeed a recommended approach) would be relatively easy
+1's	Scott Cantor, Niels van Dijk (SURFnet), Jean-François Guezou, Pieter van der Meulen
Consensus	Proceed with scoping

Group 2: Virtual Organisations and Groups

Title	**VO Assessment**
Description	Several years ago, the COmanage project put together a questionnaire aimed at helping both the VO and the organizations supporting them understand their IdM needs and business processes. This proved to be fairly useful, but it needs to be updated and expanded to help a more international audience. The old assessment is available off the COmanage wiki, hosted by Internet2.
Proposer	Heather Flanagan
Resource requirements	Minimal effort, support for a survey, and kittens
+1's	Niels van Dijk (SURFnet / GEANT SA5 VOpaas), Michal Prochazka, Slavek Licehammer (CESNET)
Consensus	Proceed

,

Title	**Focus on VOs**
Description	VOs straddle national Feds and we handle them in an ad hoc (at best!) fashion. What practices should the interfed community adopt to support their Fed/Interfed needs? Deliverables might include strawman recommended practices to national Feds and roles & responsibilities that together would define a consistent service presented to VOs. The purpose would be to inform ourselves of what it might actually take to operationalize such a service. Could build on the VO Assessment activity proposed by Heather above.
Proposer	Tom Barton
Resource requirements	A few working group members to interview principals from several VOs or other organizations that support them or otherwise are knowledgeable about needs from a VO perspective (eg, Center for Trustworthy Scientific Cyberinfrastructure). A few Fed Ops to mull this over from an operational perspective. Someone to edit a resulting doc.
+1's	Romain Wartel, Michal Prochazka, Scott Koranda, Wendy Petersen (CAF), Niels van Dijk, Heather Flanagan, Maarten Kremers (SURFnet / Geant JRA3)
Consensus	Merge with assessment activity and work with GEANT Project.

Title	**Attribute authorities and group membership/role information**

Description	Attribute authorities become interesting in VO world, where IdPs are not able to satisfy SP needs on additional attributes about the users especially group membership/roles. The main problem is when one SP wants to accept users from different VOs which use different attribute authorities. There is no common standard for representing group name/role in the attribute having VOs identification into account (just group name can lead to collision among different VOs). Some examples how group names are used by current group mgmt systems: • Perun: {vo_name}:{group_name}:{sub_group_name}:... • SufConext: urn:collab:group:{group_provider}:{group_name} Protocols which work with groups and theirs requirements on the group name: • VOOT: apart from id (usually UUID) it uses displayName which is a translatable string giving the group a human friendly name. The name is supposed to give a clear meaning for users setting up access control. • SCIM: apart from id (usually UUID) it uses displayName: A human readable name for the Group.
Proposer	Michal Prochazka (CESNET)
Resource requirements	Several conference calls should be enough for setting up the working group and produce recommendation on nameing schema for groups including VO identification.
+1's	Scott Koranda, Wendy Petersen (CAF), Niels van Dijk (SURFnet), Heather Flanagan, Tom Barton, Slavek Licehammer (CESNET), Maarten Kremers (SURFnet / Geant JRA3)
Consensus	Move to working group

Group 3: Federation Operator Best Practices

Title	**eduGAIN Recommended Practices**
Description	With edugain gaining steam, national Feds are trying different approaches to managing import, export, and filtering. This activity would review an early harvest of national Fed experiences and produce recommended practices that national Feds can use to produce a more consistent experience for IdPs and SPs, and hence for users.
Proposer	Tom Barton
Resource requirements	Perhaps 6 conference calls for a working group to organize, gather materials, net out essential recommendations. Someone to edit a resulting doc. Email list support.
+1's	Mikael Linden, Jean-François Guezou, Ann West, Heather Flanagan, Maarten Kremers
Consensus	Continuation of FOP work - frame as such. Focus on publication requirements.

Title	**Focus on R&S adoption**
Description	What is needed to jump start R&S programs in more national Feds? Produce recommendations, possibly including training, template processes and communication materials, live exchanges between Feds with established practices and others getting ready to dig into it.
Proposer	Ann West (communicated by Tom Barton, as version history will attest)
Resource requirements	Working Group with representation from a couple of national Feds already doing R&S with a couple not quite there yet. Maybe 6 conference calls and list support. Could lead to a further event programming activity.
+1's	Scott Koranda, Wendy Petersen (CAF), Ann West 😉, Andrew Cormack, Maarten Kremers
Consensus	Frame as continuing work on Entity Categories. Develop easy to consume legal opinion / cookbook. How do we assess success or failure? Tools for monitoring (see FedLab).

Title	**Contacts in Metadata**

Description	As interfederation increases in scope, so does the importance of contact information in metadata. The goal of this work group is to clarify and perhaps profile the use of contacts in metadata. Possible work items include: • Under what situations (if any) is contact information required? • What are the intended uses of specific contact types? • Clarify the use of the `mailto:` prefix. • Standardize the usage of `GivenName` and `SurName` elements in metadata. • Recommend new contact types as needed (e.g., a security contact) • Discourage the use of individual email addresses in favor of role-based email addresses (such as help_desk@example.org)
Proposer	Tom Scavo
Resource requirements	Federations have a long history of the use of contact information in metadata and so widespread agreement may be difficult to achieve but presumably the results of this working group will make it easier for entities to interfederate
+1's	Scott Cantor
Consensus	Lightweight review / survey of existing practice and report back for now.

Group 4: Alternative Methods of Metadata Distribution and Discovery

Title	**Federation at scale**
Description	Determine next steps towards dynamic resolution of entity metadata. The assumption is that this is how metadata will eventually be obtained at transaction time. This activity might focus on furthering the development and experimentation with protocols and implementations for so doing, or on how metadata comes to be sourced for dynamic resolution, or on identifying criteria by which to assess that a given dynamic resolution mechanism is working well. The purpose is to gain further experience and not necessarily to attempt anything definitive as yet.
Proposer	Tom Barton
Resource requirements	This one might have some hard resource needs. Some development. An environment in which to try things out, somehow including IdP or SP instances with which to experiment.
+1's	Lukas Hämmerle
Consensus	Scope as continuation of MDQ work lead by Ian - encourage participation in pilot of this work (including edugain).

Title	**Fresh Approaches to IdP Discovery**
Description	REFEDS has long appreciated the importance of IdP discovery in the federated model (see: REFEDS Discovery Guide). The current discovery model is dependent upon an aggregate of IdP metadata but advances in the distribution of per-entity metadata suggest that an aggregate may not always be available at the SP. A new model of IdP discovery in a world of per-entity metadata may be needed. Various approaches are possible: • continued reliance on a comprehensive aggregate of IdP metadata • a google-like, server-side search mechanism (trading latency for load time) • domain mapping eduroam-style • a client-side application or plugin The latter includes the OpenID account chooser but its relevance in this space is not well understood. The goal of this working group is to evaluate the various alternatives to IdP discovery and to recommend one or more approaches that warrant further consideration.
Proposer	Scott Cantor and Tom Scavo
Resource requirements	Note the overlap between this proposal and the proposal entitled "Federation at scale" above

+1's	
Consensus	Fold in to MDQ work.

Group 5: New Working Groups

Title	**Privacy and interfed**
Description	Is the CoCo on track? What barriers are there to its adoption? Purpose is to determine what issues a communications campaign should address to improve uptake.
Proposer	Tom Barton
Resource requirements	Working Group would conduct interviews with a selection of prospective CoCo adopting sites, blend with CoCo knowledgeable expert and a communications person to arrive at an enumeration of concerns to be addressed. Perhaps a dozen Working Group conference calls and list support. Support for a small number of group interviews.
+1's	Mikael Linden (the GEANT CoCo flywheel)
Consensus	Continue as part of Entity Category efforts (maintain standards and specifications)

Title	**Best practices for Hub-and-Spoke federation**
Description	Hub-and-Spoke federations operate a centralized authentication component as part of their Identity Federation. In Reseach and Education about 10 federations are currently running such a setup. This activity gathers best practices form those running such federations. Possible topics may include: • Operational topic, e.g. scale and security • Enduser, IdP and SP support • Trust establisment, privacy preservation and policy • Business cases for running a central component • Augmenting federation with e.g. group management, attribute aggregation, stepup authentication, credential and protocol translation and autherization • Working with metadata • Available tools and technologies • Working with eduGAIN, Code of Conduct and attribute bundles • Combining Hub-and-Spoke and Mesh federation technology
Proposer	Niels van Dijk
Resource requirements	Several conference calls, a wiki space, pehaps one or two f2f discussion meetings at existing venues
+1's	Laas Toom (EENet), José Manuel (SIR), Mads Freek (WAYF), Pieter van der Meulen (SURFnet)
Consensus	Proceed