2016 Work Plan Preparation

Please use this page to record ideas that you would like to include in the 2016 REFEDS 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! Proposals will be discussed at the REFEDS Meeting on 1st December 2015.

Want to know what was proposed in 2015? Have a look here. Want to know what was funded in 2015? Have a look here.

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

Title	Revision of SAML2int in collaboration with Kantara
Description	The soon-to-be draft-review-ready SAML v2.0 "Implementation Profile for Federation Interoperability" has a successor activity that should likely have strong participation from the REFEDS community: a revision of saml2int to freshen it and align with the implementation profile, or some different deployment profile if that is needed. A hybrid model for this activity would likely include participation from the REFEDS and Kantara communities.
Proposer	Nick Roy
Resource requirements	coordination, communication, unicorns
+1's	Tom Barton, Thomas Lenggenhager (SWITCH), Rhys Smith (UK fed)

Title	Extension of supported values for eduPersonAffiliation
Description	The eduPerson spec currently only allows a limited number of values for the eduPersonAffiliation attribute. A number of our IdPs would like to use more fine-grained values, for example to distinguish researchers from teaching staff, pre-registered students from regular affiliates, emeriti from regular alumni, etc. The eduPerson editors specifically note that "any additional values should come out of discussions with the stakeholder communities". In this activity we would coordinate these discussions, make an inventory of which values are currently in use in the different federations, and determine if we can come to an agreement to extend the set of allowed values.
Proposer	Bas Zoetekouw (SURFnet)
Resource requirements	coordination and looooots of unicorns (preferably of rainbow-dancing kind)
+1's	Jan Oppolzer (CESNET), Lalla Mantovani (IDEM), Jean-François Guezou (RENATER)

Title	REFEDS Attribute Registry

Description	The REFEDS Attribute Registry is a registry of abstract "above-the-wire" user attributes. An *abstract attribute* is used to unambiguously specify attribute requirements in deployment profiles or in SAML metadata. For example, the precise attribute requirements of the Research & Scholarship Category are: 1. `refedsNonPrivateUserID` 2. `refedsPersonName` 3. `refedsEmailAddress` Note that the concept is similar to the notion of "scope" in OpenID Connect.
Proposer	Tom Scavo (InCommon)
Resource requirements	
Comments	Nick Roy: I'd note that there probably also needs to be an IANA-level OpenID Connect scopes registry.
+1's	Nick Roy (InCommon), Nate Klingenstein (InCommon)

Title	**`OIDC profile for eduPerson attributes`**
Description	OpenID Connect (OIDC) offers an Authentication protocol similar to SAML. Many of the participants in REFEDs use the well know eduPERSON and SCHAC schema to express attributes when using SAML OIDC has a similar ability, with the use of claims. A standard set of claims is defined by OICD, however this set is not compatible with eduPERSON and SCHAC. To effectively use OIDC in R&E it would be nice if some guidelines would exist how to deal with this difference. This activity investigates the best way to deal with the differences between definitions in attributes and claims. Next to participants from REFEDs the activity will try to engage relevant parties including MACE-DIR, SCHAC and OIDC standardisation bodies
Proposer	Niels van Dijk (SURFnet)
Resource requirements	Some wiki space, a bunch of VCs, perhaps some travel budget for 1 or 2 persons.
+1's	Nick Roy (InCommon), Tom Barton, Thomas Lenggenhager (SWITCH), Scott Koranda, Jim Basney (InCommon), Roland Hedberg, Frans Ward, Maarten Kremers, Keith Hazelton (InCommon), Rhys Smith (UK fed)

Title	**`PR for Research and Scholarship Entity Category`**
Description	(Lack of) Attribute release is the single-most important issue for Service Providers. An area where this is especially hurting is in eSciences where collaborative organisations are struggling to get something, anything even, useful from Identity Providers. The technical mechanisms (Research and Scholarship attribute bundle) are in place and have been field tested by some federations. We now need a massive PR campaign to provide federations with materials to inform their IdPs and the decision makers at these institutions to release these attributes now. Extra challenge here is that the people typically involved in REFEDs are probably not the best ones to execute this work package. Out of scope for this activity are: • Discussing the R&E bundle itself
Proposer	Niels van Dijk (SURFnet)
Resource requirements	Airtime on MTV (You do remember "I want my R&S" by The Dire Straits, right?), R&S onsies, etc and perhaps some more direct marketing towards folkes within our institutions. Might also include simple marketing techniques and materials aimed at particular research areas expected to be able to start consuming federated identity on a global scale (astronomy community for example).
+1's	Jan Oppolzer (CESNET), Nick Roy (InCommon) (if I could weight my +1s, this would get top billing), Tom Scavo (InCommon), Scott Koranda (LIGO and SCG), Jim Basney (InCommon), Frans Ward, Maarten Kremers, Keith Hazelton (InCommon), Rhys Smith (UK fed)

Title	**Interfederation security**

Description	In many cases a national federation is considered as a trusted third party, who is responsible for registering and vetting entities. However, in an interfederation (like eduGAIN) there is no direct trust between the entities and the registrar. Beyond all the benefits and opportunities of such a worldwide collaboration, a couple of security questions and challenges may arise, for example: • if you cannot fully trust *every* registrar in your metadata, is it still possible to do interfederation? • what safeguards can be implemented both at interfederation and at federation level for protecting entities against rogue / abused registrars? • how to handle entityID clashes? (for scopes, see my other proposal) • what requirements are necessary for incident response? • ...
Proposer	Kristof Bajnok (NIIF)
Resource requirements	Lots of talking and writing... should it be a subgroup in REFEDs?
+1's	Tom Scavo (InCommon), Scott Koranda (LIGO), Nick Roy (InCommon), Niels van Dijk (on behalf of SURFnet), Jean-François Guezou (RENATER)

Title	**Distributed scope verification**
Description	A couple of eduPerson attributes (such as ePPN and ePSA) use scopes in attribute values to scope information to specific administrative domains. Moreover, in certain applications, scopes play a key role for authorization decisions and access control. Based on the proprietary shibmd:Scope metadata extension, Shibboleth and SimpleSAMLphp SPs are able to verify whether an entity is entitled to use a scope in attribute values or not. However, if a registrar fails to scrutinize the domain of the scope element, attackers managing to register a rogue IdP/AA entity might impersonate identities at SP software, which is one of the Worst Things. To mitigate this, it is possible to write a standard for using DNS TXT records to declare which entityIDs are entitled to a domain name in scope. Based on DNS, an SP can verify scope information more securely and without relying on the trust of the registrars. It is very much similar to the Sender Policy Framework with email.
Proposer	Kristof Bajnok (NIIF)
Resource requirements	Write RFC. Write proof-of-concept SP addons.
+1's	Tom Scavo (InCommon), Nick Roy (InCommon), Nate Klingenstein (InCommon)

Title	**Multi-federation feedback on the CIC Cloud Services Cookbook**
Description	The Committee on Institutional Cooperation (CIC, Big 10 plus) Identity Management Taskforce has created a set of best practices for vendors and IDP operators working with SaaS cloud service development/deployment. The cookbook, which can be found at https://carmenwiki.osu.edu/x/nLdCAg, is being used by, among others, Internet2 for developing TIER and Net+ standards. The document, atmidedly, has some slant toward InCommon on federation-related topics. As Interfederation grows, crafting best practices that reach beyond a single federation is increasingly important. Feedback from Refeds members on the cookbook will help adjust the current recommended best practices into something more federation-ignostic and, in turn, help those using the cookbook.
Proposer	Keith Wessel and Keith Hazelton
Resource requirements	Communications, efforts, a bit of reading time, and probably no unicorns, but a flying reindeer or eight.
+1's	Nick Roy (InCommon)

Title	**Entity Category interference coordination**
Description	There are open issues in how to interpret the presence of multiple Entity Category attributes in an IdP/SP. What does it mean than an IdP supports both REFEDS R&S and GEANT CoCo? What if an SP has both R&S and CoCo Entity Categories and wants to claim an attribute set that is less than the R&S minimum or more than the R&S maximum bundle? The rules of designing compatible ECs need to be written down so that the EC don't interfere with each other.
Proposer	Mikael Linden

Resource requirements	Maybe a face-to-face session and then write down the principles which are then blessed by REFEDS.
+1's	Roland Hedberg, Scott Koranda, Maarten Kremers, Tom Scavo (InCommon), Nick Roy (InCommon), Thomas Lenggenhager (SWITCH), Niels van Dijk (on behalf of SURFnet)

Title	**Simple SP to assist with evangelizing federated identity for research projects**
Description	A simple SP could be deployed at a simple URL (eg. my.globalsso.org) that would allow users to test if their home organization supports "global SSO"–whether or not the home organization IdP is available in eduGAIN and consumes eduGAIN SP metadata. It would not at this time test anything other than authentication. No attribute release would be tested (but if attributes happen to be released the SP could display them). Having such an SP available would be useful at scientific conferences and the like when knowledgeable community members are attempting to evangelize use of federated identity.
Proposer	Scott Koranda (SCG)
Resource requirements	REFEDs to purchase a simple domain (eg. globalsso.org) and configure DNS to point to a host that is provided and supported by a volunteer effort. Assistance with obtaining feedback from the community on the simple SP/application.
+1's	Nick Roy (InCommon)

Working Groups

We are currently assuming that the FOG, SIRTFI and OIDCre working groups will continue and the proposed ORCID working group will take shape in 2016 so no need to submit new ideas for those elements. If you would like a new WG then please submit the idea below. For more information about working groups please see the dedicated space on the REFEDS wiki.