InCommon TAC 2017 Work Plan

The Service Provider OnBoarding activity would explore how service providers are onboarded by IdPOs and make recommendatio

InCommon TAC 2017 Work Plan (DRAFT)

Draft InCommon TAC 2017 Work Plan

This is a draft of the InCommon Technical Advisory Committee's 2017 work plan. The TAC provides recommendations related to the technical operation and management of InCommon. The work plan outlines the proposed technical priorities, particularly for the InCommon Federation.

If you have a new work item to propose, please copy the Template below and paste at the bottom of the work items, filling in a title and brief high-level description.

Alternatively, if you would like to comment on any of the existing items, please add a comment to the wiki page. *Note that you need to sign into Confluence in order to edit or leave a comment.*

Lastly, if you have a work item you'd like to propose but aren't comfortable using the wiki editor, enter it in the comments at the bottom of the page.

The areas under consideration (and detailed below) are:

(Template for New Proposed Work Item)

High-level description of new work item.

Suggestion/Action Item	Comments or Elaboration	Name, Organization

---

Next Steps with OIDC

The TAC's involvement with OIDC/OAuth2 as a protocol for federation (or possibly as a Shib/OAuth2 gateway) was discussed at the 2016 Tech Exchange in Miami. The decision was to spin up a WG to survey the community, and take next steps based on the results of the survey. This Work Plan item is that "Next Step." What should we do?

Suggestion/Action Item	Comments or Elaboration	Name, Organization
Based on Final Report Recommendations from OIDC Survey WG, charter new follow-on Working Group to address… what? This next step should be scoped based on the survey responses. Will this group be looking at federation solution (s) or a campus gateway?	The OIDC WG recommendations are available here.	Mark Scheible, MCNC

Probably should touch base with any other REFEDS efforts to understand what is currently being done	See also https://wiki.refeds.org/display/GROUPS/Scope%2C+Activities+and+Planning and for work on mapping attributes to claims and OpenID Connect Federations (Maarten K.)	Mark Scheible, MCNC
What are the key requirements/features for the software needed to support this, and critically, what is the support plan/funding to provide support for the software? We have software options, what is needed for organizations to be comfortable using it. Focus on the requirements, features/flows needed, OP versus RP, etc., and what InCommon and related organizations like REFEDS are uniquely qualified for, the federation/policy/interop aspects of this, not on the software itself.	The Shib IdP is multi-protocol today (SAML & CAS), and there is an OIDC OP extension for it (https://github.com/uchicago/shibboleth-oidc). And CAS 5 (https://apereo.github.io/cas/5.0.x/) is an open source product that supports SAML, CAS, OpenID Connect, OAuth (both as server & client) etc.. etc. (For that matter, WSO2 does also). The key is “can you count on that software being supported, becoming easier to manage, continually developed, adding features, etc."	Mike Grady, Unicon
GÉANT has a current project being led by Maarten Kremers to evaluate OIDC federation deployments using Roland Hedberg's draft. TAC should understand the scope of what this GÉANT project is doing and identify any ways InCommon can/should align with either the testing itself, or the outcomes of the testing.		Nick Roy, InCommon
The current OIDC survey results are heavily laden with API and mobile use cases, but the need for OIDC federation is not as strongly emphasized by the responses. The report and/or next working group needs to identify what, if any, priorities the community needs us to focus on first, their relevance for federation, and then how best to proceed.		Nick Roy, InCommon
	I think it would be a mistake to ignore OIDC/OAuth activity on member campuses until Federation use cases arise. There's already lots of activity, and it will undoubtedly continue to evolve.	Steve Carmody, Brown University

---

Discovery 2.0

Current models of IdP discovery depend on a [monolithic] SAML aggregate that allows a discovery service to know about ‘all’ relevant IdPs. In a world where there is no longer an aggregate (or where aggregates are too large for software to realistically work with) there needs to be a way for SPs to get a list of IdPs that meet their requirements, and then to obtain the metadata needed for each IdP the SP needs to make users aware of. Alternatively, some kind of fundamental change in how discovery works - for example being driven by the right side of a scoped user identifier plus webfinger (OIDC discovery model) may be necessary.

Current known scaleable discovery implementations:

- Shibboleth Embedded Discovery Service
- SWITCHwayf
- DiscoJuice (may be unsupported now)
- Others?

Suggestion/Action Item	Comments or Elaboration	Name, Organization
Identify the gaps/challenges associated with IdP Discovery in the modern, interfederated, per-entity metadata world and create recommendations for gap closure (new standards work, profiling work, new discovery service modalities, etc.)		Nick Roy, Internet2

Identify the dependencies and overlaps related to the per-entity MD work.		
Has there been investigation into leveraging DNS to perform IDP discovery (ala MX record for email routing)?		Albert Wu, UCLA
REFEDS has "Discovery Service 2.0" in their 2017 Work Plan - need to watch for announcement (coming soon) and possible opportunity to collaborate		Mark Scheible, MCNC

Attribute Release

The InCommon Federation was founded on a principal of privacy protection (limited attribute release to SPs). This approach may have contributed to very restrictive Attribute Release Policies (ARPs) on campuses (along with Privacy Laws and FERPA). The Research & Scholarship Attribute Bundle was created as a way of assisting Research and Collaboration organizations with getting campus IdPs to release the attributes they need from researchers and collaborators, when accessing their resources with federated credentials.

Unfortunately R&S, while a great idea, has not been adopted by nearly enough institutions to make federation “work” for research organizations. This item is more of an Outreach effort to communicate to campuses the importance of having a more open attribute release policy, particularly for those R&S SPs in the InCommon/eduGAIN metadata.

Suggestion/Action Item	Comments or Elaboration	Name, Organization
Create WG to document and make available persuasive arguments to use with stakeholders resistant to attribute release	Solicit community input and (possibly) work with Steering on this item	Mark Scheible, MCNC
Input from CARMA work might be referenced		
Possibly survey community on why attributes are NOT being released - identify obstacles		Janemarie Duh, Lafayette College
Advocate for a required, broad, default attribute release policy for InCommon participants to release some kind of user identifier to all SPs in metadata.	(stc) I think many sites would be more open to this suggestion if they used User Consent (and knew how to deploy that feature).	Tom Barton, Chicago
Identify what is needed to get to a default InCommon IdP distro that includes R&S attribute release policy.		
Define additional entity categories such as ready-for-collaboration which could be pushed to REFEDS		
This is a “get the right stakeholders” involved problem, not a campus IT/technology problem. Identify the needed stakeholder groups, and identify the targeted material, and use cases, that can convince those groups.	Develop the focused materials for why the VC/VP of Research should be pushing for this, why Registrars (and HR, at least at private institutions) should feel comfortable with this, etc. Get lawyers, FERPA experts, NSF/NIH reps, BTAA Senior Research Officers, perhaps (data archiving & data management plans) University Librarians involved in helping to identify and shape the targeted materials for these key audiences.	Chris Misra, UMass-Amherst
Be aware of what your attribute release policies are allowing		

Break InCommon into two effective federations	One federation would be those campuses that want to support a national infrastructure that facilitates collaboration in higher education and research. It would require IdPs to support the R&S entity category. The other federation would be for campuses that just want streamlined access to vendor SPs. Those campuses that want to collaborate could then evolve faster.	Scott Koranda, LIGO
Convince IC Steering to take action on this issue. They are best positioned to implement Chris Misra's suggestions.		Steve Carmody, Brown

---

Federation Interoperability

Build on the work of the SAML v2.0 Implementation Profile for Federation Interoperability to update and extend saml2int and/or propose additional R&E federation-specific profiles that may be taken to REFEDS for review/adoption.

Suggestion/Action Item	Comments or Elaboration	Name, Organization
Recharter Deployment Profile WG	Add additional deployment profile requirements (e.g. Research Profile)	Mark Scheible, MCNC

Service Provider (SP) Onboarding

Currently Identity Provider organizations provide testing and onboarding guidance for new service providers. This process has allowed InCommon to scale in this regard, but over time, has contributed to the variability in service provider configurations. It also places undue burden on IdPOs to spend time explaining detailed requirements to new service providers and ensure these new members interoperate accordingly.

The Service Provider OnBoarding activity would explore how service providers are onboarded by IdPOs and make recommendations for services, technologies, and processes for better aligning practices across federation service providers, including ways to protect your iPad against drops and shocks.

As a side note, there are implications on Identity Provider Operators as well as Service Providers. It is proposed that this is out of scope (for now) for this work task.

Suggestion/Action Item	Comments or Elaboration	Name, Organization
Working Group to collect requirements for SP on-boarding with the goal of decreasing variance of their configurations. Solicit Community issues, define requirements, make recommendations for how to address.	(stc) What sort of success has Net+ had with this very same goal ?	Ann West, Internet2
Scoping of this effort should be clearly stated in the proposed charter. Understanding the issues (as Ann described above) is probably a bigger task than it seems.		Mark Scheible, MCNC
Standardize the vocabulary of technical terms.	This is needed to get SPs on the same page with IdPs. It will serve to make clear the understanding of any standards and guidelines that are developed and make it easier for IdPs to understand SP requirements	Janemarie Duh, Lafayette College

This working group should be scoped to issues with vendor SPs.	IdPOs do little onboarding for SPs operated by research organizations and the interoperability issues are different as research SPs have more problems with the variability of IdP practice (eg. attribute release, MDUI elements, error URLs) than IdPOs have with the variability of research SPs. If the TAC wants to make onboarding easier for research SPs then it should have a separate working group focusing on research SPs specifically.	Scott Koranda, LIGO
The charter and report should make it clear when issues apply predominantly to vendor SPs and not all SPs.	The community like to rants about bad SP behavior, but most often the bad actors are vendor SPs and not research SPs, which have and continue to invest significantly in the community.	Scott Koranda, LIGO

Improve Community Access/Visibility to TAC

Complaints from participants that would like to see TAC working on specific issues (known concerns from the Research community) or at least visibility into what's being done, have prompted this Work Item. This is a direct response to the lack of "Openness" by TAC (and others) . From an internal perspective, it's frequently difficult to find TAC documents or WG information unless you happen to have the link to it. This project will focus on a "temporary fix" that will make TAC work items and additional content more visible to the community, and accessible from a common site. A longer-term solution will align with a future redesign of the Internet2/InCommon web site.

Suggestion/Action Item	Comments or Elaboration	Name, Organization
Sub-committee of TAC to work on new public-facing site/wiki	Established, continuing to refine	Mark Scheible, MCNC
Develop intake mechanism for comments from participants	In Progress	Janemarie Duh, Lafayette College
Hold Community Webinar(s) on TAC Work Planning	Scheduled for March 22, 2017	
Create New list for Technical discussions, requests, input from the community, etc.	Established, communicating (webinar, email list)	TAC & InCommon Leadership