Un-Affiliated IdP Working Group Draft Annual Report, 2017

Problem Statement

Service Providers (SPs) often f-ind that the population they want to serve includes individuals who are not represented by campus-based or other institutional Identity Providers (IdPs). In other cases, the individual's organizational IdP can not (or will not) release attributes necessary for the operation of the SP. The two most commonly encountered accommodations for users in this situation both suffer from serious inadequacies. First, SPs can opt to issue credentials and run an authentication service for those users lacking an adequate federated solution. The drawback is that this forces the SP owners to take on the unwelcome role of issuers and managers of user credentials. It is not their core mission and it can easily become a substantial support burden. The second fallback is to accept external IdPs such as Google. This gets the SP owners out of the credential management business, but brings other issues. To take Google as an example, Google's IdP-like service comes with several caveats: Their business model is premised on monetizing user and usage data; As a non-SAML solution, they don't support the Enhanced Client or Proxy (ECP) Profile, a critical requirements for some key research services; They also reserve the right to throttle usage if it gets above what they consider an acceptable level of use.

A different approach is clearly needed. Ideally, individuals lacking a suitable IdP could be invited to register with a participating IdP that offered no-cost, easy self-registration processes. This REFEDS IoLR Working Group is charged with specifying how such a service should be structured and establishing processes by which Research and Education groups may identify potential "Un-Affiliated IdPs", or informally, "IdPs of Last Resort". For some additional background, see the 2015 *Final Report* of the InCommon Technical Advisory Working Group, IdPoLR.

Goals and Deliverables

- A checklist of requirements and features that would qualify an IdP as an Un-Affiliated IdP
- A self-assessment tool by which IdPs may rate their service agains the checklist of requirements
- A publicly available registry of IdPs that have completed the checklist that includes their responses
- A REFED-scale communications plan about the service and how to connect with it
- Add participation in SIRTFI (federated incident handling agreements) to the checklist for Un-Affiliated IdP services
- Promote the practice of users establishing accounts with more than one self-declared Un-Affiliated IdP
- Define processes by which an SP may register multiple identities for a given user from multiple Un-Affiliated IdPs.
- Work with REFEDS and the community of Research and Education Service Providers to insure the long-term availability of Un-Affiliated IdP Services.