IdPoLR Working Group Final Report

Executive Summary

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 working group was chartered to determine the characteristics of a fully adequate solution to this challenge and to make recommendations on the steps that would be involved in implementing that solution. The envisioned answer is an "IdP of last resort" that serves users otherwise unable to access specific services. Historically, ProtectNetwork played this role, but their business model shifted over the years to the point that the cost of ProtectNetwork's services has become financially prohibitive for many SPs. Past usage of ProtectNetwork did, however, clearly demonstrate the appeal of an IdP of last resort: A few years ago, something on the order of 40% of logins to the Internet2 wiki were accomplished with ProtectNetwork credentials.

While the problem potentially applies to any federated service, the working group was explicitly directed to focus on identifying and responding to the needs of service providers in the research and scholarship (R&S) space, including but not restricted to cases that leverage the international R&S entity category. The present working group report spells out the requirements that an IdP service needs to meet to qualify as a full solution to the R&S challenge. The report closes by recommending concrete courses of action that InCommon could take to foster the emergence of a service meeting all the documented requirements.

In addition to the present report, the working group also drafted individual evaluations of a small number of candidates for an IdP of last resort service. These evaluations will be shared with InCommon after it is determined if there is interest in moving forward.

Scope and Limits of the Proposed Service

The Research & Scholarship (R&S) category of services are a class of services that are likely to require an IdP of Last Resort. However, none of the available IdPs in the InCommon Federation meet all the requirements of the R&S community. What is needed is an IdP of Last Resort specifically addressing this service gap.

To illustrate how this plays out, take the following example from R&S. As each new R&S SP comes online, it must address the gaps in coverage of the SP's user community by InCommon R&S IdPs. The lack of an IdP of Last Resort (IdPoLR) offering by InCommon requires the SP to choose a non-InCommon solution to this problem. Typically the SP decides to use local user passwords and/or Google logins, and the SP either makes InCommon logins a secondary option or decides that InCommon integration isn't worth the additional effort and so doesn't register with InCommon at all. Since new R&S SPs come online all the time, availability of an InCommon IdPoLR is an urgent need for growing InCommon's relevance in the research community.

An "IdP of Last Resort" is, as the name suggests, only intended as a last resort and is not intended to take the place of an organizational IdP. Having an IdP run by an organization with which the user is affiliated, and which meets the user's needs in interacting with SPs, is clearly the desirable state for all users.

It is our implicit recommendation that InCommon continue to make it very plain to its participants that, if they are not doing so already, they should endeavor to run an IdP for its user community that is managed in such a way as to meet their needs. For example, if organizational policy is preventing the IdP from releasing attributes that the user needs to access R&S SPs, then the policy should be revisited in that light, and/or a clear and flexible exception process implemented. Users should use their organizational IdP unless:

- the organization doesn't have an IdP
- the organization's IdP doesn't release required attributes to the SP
- the SP requires ECP but the organization's IdP doesn't support ECP
- the SP requires MFA but the organization's IdP doesn't support MFA

Generally the user can and will use the organizational IdP for most SPs but due to attribute release policy constraints, or an unmet need for ECP or MFA, the user may find it necessary to use the IdPoLR with a few SPs. In sum, using the IdPoLR should be the exception, not the rule.

Requirements from Research and Scholarship SPs on an IdP of Last Resort

1. The IdP must support the R&S entity category and be tagged as such (Note: Requirements 2, 3 and 4 are implied by the terms of R&S).
2. It must have the ability to Assign/Assert ePPNs.
3. It must have the ability to Assign/Assert ePTIDs or provide a SAML2 persistent NameID if ePPNs are re-assignable.
4. It must accept SP requests for authentication contexts via the standard SAML2 Authentication Request Protocol.
    a. This is for InCommon Bronze, as well as Silver and MFA, if supported.
5. It must support SAML Enhanced Client or Proxy (ECP).
6. It must support user self-registration in a manner that lets the user know what, if any, further steps are required before they can authenticate to the SP they were initially trying to access.
7. User sessions at the IdP should have a reasonable default duration, allowing multiple SPs to leverage the same user session when that is appropriate to the context.
8. The IdP operator must address the service longevity issue (even if for now the response is "TBD").
9. It must support Recommended Technical Basics for IdPs (as of May 2015, with future development of the recommendations accommodated as possible, and in negotiation with InCommon).

10. It must conform to the 'Interoperable SAML 2.0 Web Browser SSO Deployment Profile' as documented at http://saml2int.org (as of May 2015, with future development of the recommendations accommodated as possible, and in negotiation with InCommon).
11. It must be certified for InCommon Bronze.
12. The IdP must have no commercial interest in the use of user data.
13. The IdP should, by design, be a service available to any R&S SP needing an IdPoLR, assuming the SP's federation supports R&S and eduGAIN.
14. There must be no charges to the user for use of the IdPoLR service.
15. The IdPoLR service shall employ techniques to minimize system failures and ensure that any failures are not likely to result in inaccurate Assertions being sent to SPs.

The following criteria are highly desirable, but not required.

1. Publishes aggregate usage statistics to give feedback to campus IT on use by their constituency (i.e., motivate campus to participate in R&S so the campus users don't need the IdPoLR anymore)
2. Support for user consent
3. Support for Silver credentials and authN (to be combined with local identity vetting to achieve Silver LoA)
4. Low/no cost to SPs for use
5. Accepts non-ASCII characters (e.g. uses UTF-8 as the default encoding) in user-entered data
6. Support for some form of multi-factor authentication that is low/no cost for users

Risks and Their Mitigation

Risk	Mitigation
Loss of incentive for institutions to support R&S and its associated attribute release policy.	Foster better understanding by campus leadership of how essential it is to support the research communities' needs with regard to federated identity. The Scope and Limits section above provides additional background on this topic.
Potential users will be unaware of the option to use IdPoLR.	Research SPs actively market the option to their users and make it easy to use
If InCommon launches a trial service and at the end of the trial it is decommissioned, users & SPs could be orphaned.	Lower the risk of service decommissioning by fostering adoption and use of the IdPoLR service and working together to develop a plan for service sustainability.
If InCommon waits until we have the perfect service, the Research SPs will have found one or more non-InCommon solutions.	Roll out an initial version of the service as soon as feasible.
Self-registration without additional requirements around identity proofing would not satisfy the security concerns of R&S SPs.	Add identity proofing steps to a post 1.0 version of the service. In the meantime, it is our understanding that many research organizations vet identities of their remote users through out-of-band means. In such cases the SP admins are relying only on the IdP's assertion that user x controls a set of authentication credentials (i.e. they successfully authenticated). If the SP admins have established to their satisfaction through other means that the person controlling those credentials is someone known to their community, the admins may have mitigated, to their satisfaction, the risk implied by the IdP's low/zero level of ID proofing. If the process involves some form of stronger authentication, such as the use of two factors, the risk that the credential is under the control of someone other than the original holder is mitigated to a further degree.

Recommendations

Short and Long Term Recommendations

In recent years InCommon has expressed interest in offering stronger and more direct support for the research mission of member campuses and virtual organizations. One of the more concrete ways to back this up with action in the near term would be for InCommon to help bring into existence an IdP of Last Resort that meets the needs of R&S service providers. Therefore, our primary recommendation is that InCommon take steps to help make available a production IdPoLR service. An IdP meeting all these requirements is unlikely to appear through spontaneous generation. On the other hand, InCommon does not necessarily need to operate the IdP in question, it may be enough for InCommon to identify and support the launch of an independent service

operator. Any near-term solution should initially offer a basic set of identity provider services. A solution meeting the requirements detailed above would provide that basic set of services The suite of services could be expected to grow over time as needs evolve and resources permit.

It is worth noting that requirement 12, "No commercial interest in the use of user data" does not rule out commercial service providers as IdPs of Last Resort, but it does rule out those who seek to monetize the user data they collect.

In addition to recommending a near-term plan to get an IdPoLR service into production as quickly as possible, the working group recommends beginning work on a longer-term plan to create a level playing field for any potential provider to offer a comparable or better service. The urgency behind the short-term recommendation comes from the research service providers who have a critical unmet need to enable all of their potential users to access their research sites and tools. The long-term value of encouraging the emergence of multiple IdPs that meet this requirement is to mitigate the risk that failure of a single IdP would mean the end of the service as a whole.

Having a clear set of requirements is one important prerequisite to creating a level playing field on which multiple IdPoLRs can play. Another is some form of tagging of IdPoLR services. One of the ways to meet both of these prerequisites would be by leveraging emerging practices in the entity category space. The REFEDS Research and Scholarship Entity Category specification (http://refeds.org/category/research-and-scholarship) provides a concrete example of this approach in action. The requirements and conditions on qualifying services would be spelled out in the document formally defining the category. It would likely have to be managed as a self-asserted tag by IdPs who would commit themselves to meeting all the requirements. An alternative would be to have a federation register and vet candidate IdPs. However, that would place an onerous burden on the federation which would have to define a set of processes and devote staff time to the registration, vetting and marking of IdPoLRs. Another alternative would be for some organization representing R&S service providers to maintain a list of qualifying IdPoLR services. Regardless of this, nothing would prevent an individual R&S SP from making it's own determination of which, if any, IdPoLRs it would accept.