Deprecated draft on candidates for an IdPoLR service

Near Term and Possible Longer Term Candidate Services

The working group recommends working with the non-profit UnitedId (unitedid.org) to roll out an initial version of the defined IdPoLR service. We see no other ready candidates in the non-commercial space. Could the R&S needs be met by an existing external IdP offered by a commercial company? Such a solution would fall short of meeting several of the mandatory requirements: 1) Most obviously it would not be able to truthfully proclaim that it has no commercial interest in the use of user data; 2) Unless it becomes a member of an existing identity federation, it would not be able to qualify as an R&S-supporting IdP or be certified at federation-defined levels of assurance such as InCommon bronze; 3) It would not support ECP; and 4) With one possible exception it could not provide a suitable identifier: None of the known providers guarantee non-reassignability of usernames for supplying an ePPN and only one offers a directed identifier (like ePTID) as an alternative. A social-to-SAML gateway could be designed to mitigate many of these deficiencies, but it would not be a straight-forward or issue-free effort to come up with such a design.

Alternatives to recommended solution

We also investigated the extent to which existing or planned identity provider services within InCommon could meet the mandatory requirements. The certificate manager application and the federation manager application use an Multifactor IdP Proxy combined with a social-to-SAML gateway to serve administrators who do not (yet) have a home IdP. There are plans to supplement this with a native IdP service to address cases where users don't want to use commercial identity providers and have no home IdP. This "embedded IdP" could theoretically be enhanced to act as an IdP for R&S SPs, but that is several technical steps and a few major service portfolio decisions away from realization.

Looking longer term, the TIER initiative is committed to address a number of gaps in identity and access management and an IdPoLR service might be considered one of those gaps, but the TIER effort is at the requirements gathering stage, and development priorities are yet to be defined.

Assessment of recommended solution with respect to defined requirements

The near-term solution should initially offer a basic set of identity provider services. The suite of services could grow over time as needs evolve and resources permit. Here is an assessment of UnitedId against the requirements defined above:

UnitedId meets the following MUST requirements today:

- Support for user self-registration (but see first bullet under 'some dev. work needed' below
- Once user has authN (there is an SSO session)
- Ability to assign ePPN (these are non-reassignable)
- Accepts SP requests for authentication contexts via the standard SAML2 Authentication Request Protocol
- Support for Tech Basics for IdPs
- Conforms to saml2int
- No commercial interest in the use of user data (by organizational principle, backed by support of Code of Conduct)
- Available to users throughout the world

By joining InCommon and taking a set of procedural steps, UnitedId could also meet the following MUST Requirements

- IdP must support R&S
- Support for ECP (already on UnitedId roadmap under near-term goals)
- InCommon and UnitedId will work together to define approaches to service sustainability, but the first goal is to get an initial IdPoLR in service and in use
- Self assertion of bronze
- IdP must be available globally to any R&S tagged SP (both InCommon and Refeds R&S for now)

Some development work would be needed to meet the remaining MUST Requirement

- In case user is a first-time registrant at UnitedId, an appropriate SAML error message is returned to the SP so that the user is not stranded between IdP and SP, but is returned to the SP where the error can be handled gracefully. (DHW: This isn't one of the MUSTs, as far as I can see.)

UnitedId also meets the following desired conditions:

- Support for user consent
- Accepts non-ASCII characters in user-entered data
- Supports multi-factor authN
- No cost for users* *if they have a smart phone, or SP subsidizes other 2nd factor

Steps Entailed if Recommendation is Accepted

If InCommon endorses the primary recommendation and chooses to move ahead toward a UnitedId-based IdP of Last Resort, the next steps would include the following:

- Open discussions with UnitedId to come up with a mutually agreed-upon set of terms and conditions to launch an IdPoLR and maintain it for a stated period of time (do this in consultation with key R&S SP stakeholders)
- Arrange for UnitedId to become a member of InCommon
- Have this IdPoLR designated as supporting R&S (both InCommon and Refeds R&S definitions)
- Authorize this IdPoLR to assert compliance with InCommon Bronze level of assurance