Rationale for Required and Desired Features in the IdP of Last Resort Working Group Report

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

R1. 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).

One of the primary barriers that providers of Research Services encounter is that the Identity Providers available to many of their users do not, and in many cases will not, release the minimal set of attributes that they need for many of their use cases. It is precisely in those cases that an IdP of Last Resort becomes a possible solution--but only if the IdP of Last Resort DOES release that minimal set of attributes. An IdP marked with the R&S (Research and Scholarship) entity category has agreed to release a standard set of attributes to any service provider that also carries the R&S tag. The R&S tag is assigned to an SP by the InCommon (and other) federations only if the service it provides fits the Research and Scholarship definition.

Basically, this requirement guarantees that a research SP can count on the fact that an IdPoLR will provide them with the attributes they need without the need for ANY prior bilateral arrangements between them.

R2. It must have the ability to Assign/Assert ePPNs.
R3. It must have the ability to Assign/Assert ePTIDs or provide a SAML2 persistent NameID if ePPNs are re-assignable.

Service providers need a single consistent primary identifier to key off all information about a person. If this key changes, or the same key is subsequently assigned to a different user, then the original person's settings, history, and related data are lost to them. Requirements R2 and R3, taken together, guarantee that a suitable identifier will be available to the SP.

R4. It must accept SP requests for authentication contexts via the standard SAML2 Authentication Request Protocol.

a. This is a requirement for InCommon Bronze Identity Assurance profile, as well as the related Silver Profile and multi-factor authentication, if supported.

To support a higher level of assurance of identity for higher risk or higher value services, an SP needs a way to signal to the IdP that it needs a particular level of authentication. The Security Assertion Markup Language (SAML) protocol defines a way to signal the need for a specific authentication context. Requirement R4 obliges the IdP of Last Resort to support this part of the SAML protocol. When the US Government begins requiring Assurance profile support for credentials, the Identity Provider will be able to provide them.

R5. It must support SAML Enhanced Client or Proxy (ECP).

Without support for the Enhanced Client or Proxy (ECP) profile of the SAML specification, IdPs are only capable of supporting browser-based applications. However, many research applications and services are only accessible via command line tools. The ECP profile defines a way that SAML can be used in such scenarios, thus meeting a common requirement in research environments.

R6. 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.

Research SP operators have noticed that in many cases, when a new user first visits the SP, and is sent off to register at an IdP, the user experiences an unexplained failure, and may simply be left waiting for a response that never comes. If the IdP of Last Resort can at least signal back to the SP that, for example, the user has to perform other steps before their registration is complete, then the SP can at least provide the new user with a meaningful explanation of what has happened.

R7. 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.

This is basic WebSSO good behavior. If the IdP session times out while a user is at one SP, and the user then invokes a second application, they will be forced to re-authenticate with the same IdP, thus violating the user's expectation of how single sign-on should work.

R8. The IdP operator must address the service longevity issue (even if for now the response is "TBD").

One of the more difficult challenges facing users of an IdP of Last Resort service is sustainability over time. By including requirement R8, this issue is put in the foreground at the very beginning of the process so that both the SPs and the IdPs have an understanding of the importance of sustainability.

R9. 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).

R10. It must conform to the 'Interoperable SAML 2.0 Web Browser SSO DeploymentProfile' as documented at http://saml2int.org (as of May 2015, with future development of the recommendations accommodated as possible, and in negotiation with InCommon).

If the IdP of Last Resort meets requirements R9 and R10, it will go a long way toward achieving out-of-the-box interoperability with well-configured SPs. Setup can be much more painful and time-consuming if there are interoperability issues.

R11. It must be certified for InCommon Bronze.

We know that support for higher levels of assurance will be required for certain research SPs. By requiring support for Bronze, the lowest category of assurance, the IdP of Last Resort will at least be well positioned to support higher levels of assurance when the need arises.

R12. The IdP must have no commercial interest in the use of user data.

A researcher should not have to accept the monetization of their personal data by any party as a condition of getting access to needed research services.

R13. 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.

The research community is global by its very nature, so the IdP of Last Resort should be an option for SPs regardless of their location. Otherwise, we will not solve the original problem.

R14. There must be no charges to the user for use of the IdPoLR service.

If there are charges associated with a researcher's use of the IdP of Last Resort, some percentage of them will simply refuse to use it, thus thwarting the SPs goal of making their service available to all its potential users. Further, many projects funded by national agencies such as the National Science Foundation cannot operate in a mode where users must pay a fee to access the project's resources.

R15. 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.

Requirements R15 speaks to the need for the IdP of Last Resort to provide reliable and trustworthy service.

The following criteria are highly desirable, but not required.

D1. 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)

Some people have expressed concern that the existence of an IdP of Last Resort will be seen by some campuses as an alternative to a campus-provided IdP that serves the institution's research mission. D1 would provide information that could be used to identify the level of demand for a campus-level solution.

D2. Support for user consent

Now that there are SAML implementations that support user consent to attribute release, this will become a best practice. D2 is meant to encourage the deployment of user consent functionality.

D3. Support for Silver credentials and authN (to be combined with local identity vetting to achieve Silver LoA)

There are research services and resources that will only be accessible to users who can provide a higher level of identity assurance. Users can only do that through IdPs that are capable of selectively guaranteeing the required level of assurance.

D4. Low/no cost to SPs for use

Research organizations' budget for support services is never overly-generous, so it is desirable for infrastructure costs, like identity and access management, to be kept to a minimum.

D5. Accepts non-ASCII characters (e.g. uses UTF-8 as the default encoding) in user-entered data

ASCII-only is not a good choice if the goal is to welcome and support a global research community.

D6. Support for some form of multi-factor authentication that is low/no cost for users

Multi-factor authentication can be an important component in raising the SPs assurance that their users are who they claim to be. As high-value resources are put online, the need for higher assurance will increase.