[This comparison was supported by ORCID. Please use freely as a resource, though, note that the table content may be protected by their referenced owners.]

The community has been creating a group of requirements for Identity Providers of Last Resort (IdPoLR / IoLR). These Identity Providers would be used by Service Providers when one or more users do not have access to authentication/ authorization credentials via their home institution. The resulting requirement from two efforts are compared below. The requirements for these two efforts are from the following documents:

A. 2015 InCommon IdPoLR Working Group Final Report:
Requirements from Research and Scholarship SPs
https://spaces.at.internet2.edu/display/IDPoLR/IdPoLR+Working+Group+Final+Report

B. 2018 REFEDS IoLR Working Group Declaration and Self-Assessment form:
Unaffiliated IdP Requirements
https://docs.google.com/spreadsheets/d/1U1A8kfpumGnFydPNVuBnf2dZD4XJzwEwp6Yfq2-3PHs/edit#gid=0

A. Requirements from Research and Scholarship SPs	B. Unaffiliated IdP requirements
1. The IdP must support the R&S entity category and be tagged as such Implies requirements 2, 3, and 4 from the list: ● It must have the ability to Assign/Assert ePPNs. ● It must have the ability to Assign/Assert ePTIDs or provide a SAML2 persistent NameID if ePPNs are re-assignable. ● It must accept SP requests for authentication contexts via the standard SAML2 Authentication Request Protocol.	1. The IdP supports the Refeds R&S entity category and is tagged as such
5. It must support SAML Enhanced Client or Proxy (ECP). *[ECP enables client sign in without a browser, such as for desktop applications, or server-side code running in a web application]*	2. The IdP supports 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.	3. The initial registration flow leave the registrant with clear expectations as to their next steps
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").	4. What is the IdPs sustainability plan for production-level IdP service operation

A. Requirements from Research and Scholarship SPs	B. Unaffiliated IdP requirements
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).	
	5. The IdP publishes a service description and roadmap
10. It must conform to the 'Interoperable SAML 2.0 Web Browser SSO Deployment Profile'	6. Conforms to the Kantara-hosted SAML Federation Interoperability Profile
11. It must be certified for InCommon Bronze. *[an authentication assurance level, equivalent to NIST AL1]*	
	13. The IdP supports assurance levels equivalent to NIST AL2 or above
12. The IdP must have no commercial interest in the use of user data.	7. The IdP has no commercial interest in the sharing of user data with other parties
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.	10. Any SP in eduGAIN may request to use this IdP
14. There must be no charges to the user for use of the IdPoLR service.	8. The IdP does not charge its registrants for services
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.	
	9. Anyone may register at this IdP
	11. The IdP meets SIRTFI criteria for federated incident response handling.
	12. The IdP supports one or more forms of Multi-Factor Authentication.
	14. The IdP a. Accepts Authenitcaiton Context requests b. Supports the standard comparison methods c. Does not return an Authentication Context if it can't meet the stipulated criteria