REFEDs Review of the InCommon IdP of Last Resort WG Requirements

#	InC requirement	Refeds Restatement or Comments	Status	Notes
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).	"The IdP must support the Refeds R&S entity category and must be tagged as such."	Approved	
2	It must have the ability to Assign/Assert ePPNs.	See #1	Approved	
3	It must have the ability to Assign/Assert ePTIDs or provide a SAML2 persistent NameID if ePPNs are re-assignable	"If ePPNs are reassignable by the IdP, it must provide a SAML2 persistent NameID or an ePTID, preferably the former."	IOLR review	
4	It must accept SP requests for authentication contexts via the standard SAML2 Authentication Request Protocol. ▪ This is for InCommon Bronze, as well as Silver and MFA, if supported.	"The IdP must accept authentication requests that include one or more requested authentication contexts and that may include a comparison method for evaluating the requested context classes or statements. If a comparison method is absent or "exact" and the IdP cannot satisfy the requested authentication context it must indicate no authentication context in its reply."	IOLR review	
5	It must support SAML Enhanced Client or Proxy (ECP)	"It must support SAML Enhanced Client or Proxy (ECP)"	Approved	
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.	"The initial registration flow should leave the registrant clear as to the next steps and avoid a user experience that ends with an inexplicable error or process termination. This applies whether the flow is SP first or registration first."	IOLR review	
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.	Drop. A basic feature of federated IdPs.	IOLR review	
8	The IdP operator must address the service longevity issue (even if for now the response is "TBD").	This is a matter for the community to address and is one of the reasons we encourage multiple IdPs to support the Un-Affiliated IdP requirements.	IOLR review	
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).	That document has been superceded by the Kantara Initiative draft, "SAML V2.0 Implementation Profile for Federation Interoperability", https://kantarainitiative.github.io/SAMLprofiles/fedinterop.html. Open Question: What is the relationship between REFEDs and the Kantara Initiative? The IOLR Working Group should review the Kantara draft and offer suggested revisions. The ultimate goal should be to make compliance with this implementation profile a condition for designation as an Un-Affiliated IdP.	IOLR review	
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)	See #9	IOLR review	
11	It must be certified for InCommon Bronze.	A lot has changed since InCommon Bronze and Silver were defined. How should federations address the issue of levels of assurance?	IOLR review	
12	The IdP must have no commercial interest in the use of user data.	"The IdP must have no commercial interest in the use of user data."	IOLR review	
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.	"Any SP that has users in need of an Un-Affiliated IdP should be able to advise them to register with one with the expectation that the IdP will agree to authenticate its users to the SP."	IOLR review	
14	There must be no charges to the user for use of the IdPoLR service.	"There must be no charges to the user for use of the IdPoLR service."	IOLR review	
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 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."	IOLR review	
X1	Practicing member of SIRTFI		IOLR review	