Requirements for an IdP of Last Resort

The following list of requirements has stabilized over the last several months. Comments are welcome.
(NOTE: numbering is for reference convenience only, and is not intended to denote prioritization)

1. Support for user self-registration
    a. User registration incorporated into sign-in flow, so new user is not stranded at IdP
    b. User registers once for sign-in to multiple Research and Scholarship (R&S)-tagged SPs (i.e., user identity is not SP-specific)
2. Once user has authenticated at the IdP, user is not prompted for password again when visiting other SPs during the same browser session, unless required by the SP
3. IdP must support the R&S entity category and be tagged as such
4. Ability to Assign/Assert ePPN; values must not be reassigned
5. Ability to Assign/Assert ePTIDs
6. Must address the service longevity issue (even if for now the response is "TBD")
7. Support for SAML Enhanced Client or Proxy (ECP)
8. Support for Multiple AuthN Contexts for MFA and Assurance
    a. This is for their InCommon Bronze, as well as Silver and MFA, if supported.
9. Support for Recommended Technical Basics for IdPs
10. Conforms to the 'Interoperable SAML 2.0 Web Browser SSO Deployment Profile' as documented at http://saml2int.org
11. Self-assertion of InCommon Bronze compliance
12. No commercial interest in the use of user data
13. IdP must be available globally to any R&S tagged SP
    a. NOTE: This can only be achieved at the federation level, not unilaterally by an IdP
14. Available to users throughout the world (perhaps with invitation from "approved" projects)

The following criteria are highly desirable, but not required.

21. 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)

22. Support for user consent

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

24. Low/no cost to SPs for use

25. No cost for users

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

27. Support for some form of multi-factor authentication