Near-term Candidate IdP of Last Resort Service: UnitedId.org

If InCommon chooses to adopt the IdPoLR Working Group's recommendation to help make available an IdPoLR service as soon as possible, then UnitedId.org would be a strong candidate. That claim is based on the following evaluation of UnitedId against the requirements defined in the WG's final report.

UnitedId meets the following MUST requirements today:

- Support for user self-registration (but see first bullet under 'some dev. work needed' below)
- Once a user has authenticated an SSO session is established at the IdP
- 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 would 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

- User registration incorporated into sign-in flow, so new user is not stranded at IdP. NOTE: In case user is a first-time registrant at UnitedId, the second factor issuance/registration process will not be instantaneous. In such cases, 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.

UnitedId also meets the following desired conditions:

- Support for user consent
- Accepts non-ASCII characters in user-entered data
- Supports multi-factor authN (MFA)
- 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
- Develop a communication plan to inform R&S SPs (and users) of the availability and purposes of the service