Requirements for an IdP of Last Resort

9-December-2014

The InCommon TAC created a subcommittee tasked with developing requirements for an IdP of Last Resort for use by R&S SPs. One of the drivers for this effort is the desire to replace the functionality currently provided by ProtectNetwork, which has a fee structure that has become unacceptable for certain R&S SPs.

Below is a non-ordered list of requirements resulting from the work of the subgroup.

- Support for user self-registration
  - User registration incorporated into sign-in flow, so new user is not stranded at IdP
  - User registers once for sign-in to multiple R&S SPs (i.e., user identity is not SP-specific)
- 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.
- IdP must support the R&S entity category and be tagged as such
- Ability to Assign/Assert ePPN; values must not be reassigned
- Ability to Assign/Assert ePTIDs
- Must address the service longevity issue (even if for now the response is "TBD")
- Support for ECP
- Support for Multiple AuthN Contexts for MFA and Assurance
- Support for Recommended Technical Basics for IdPs
- Self-assertion of InCommon Bronze compliance
- No commercial interest in the use of user data
- IdP must be available globally to any R&S tagged SP
  - NOTE: This can only be achieved at the federation level, not unilaterally by an IdP.
- 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)
- Available to users throughout the world (perhaps with invitation from "approved" projects)

The following criteria are highly desirable, but not required.

- Support for user consent
- Support for Silver credentials and authN (to be combined with local identity vetting to achieve Silver LoA ?
- Low/no cost to SPs for use
- Language agnostic (capability for UI localization?)
- Support for some form of multi-factor authentication