External Identities Work Group Meeting - 2015-03-26

Agenda

Agenda will be reviewing/discussing the updated draft of the External ID Report draft at:

- https://docs.google.com/document/d/1IVDjmdCqToB9aGAlF5SVLCmVHskCqmtN7kW_jRhOWPs/edit?usp=sharing

Pre Meeting Notes

distributed with agenda

There has been substantial editing and reorganization since our last meeting, so probably a little more than a “quick scan” will be needed to digest it, even if you’ve read the previous versions carefully.

Main editing efforts:

- Reorganized several topics
- Shortened many sections headers. (No line wraps in the ToC! :))
- Consolidated definitions of identity, attribute, credential, linking even further in first sections
- Added a new section on “Trustworthiness of external identities”
    - (which thinking about it is more about “how much you will trust” them than “how trustworthy they are implicitly”)
    - Added a section on considerations when leveraging external *credentials* in lieu of institutional ones.
    - Reorganized the “Architecture” section to remove the strong focus on “Gateways” and instead focus on the services gateways can provide (but that can also be provided in other forms than gateways).
    - Put in more discussion of targeted vs “global” identifiers from external identities
        - Text was added in the “Definitions” section and also in several areas of the “Architectural Approaches” section
        - Edits to the Evaluating External Identity Providers (https://spaces.at.internet2.edu/display/EXTID/Evaluating+External+Identity+Providers) matrix to make it more appropriate for linking from the report.

Topics previously discussed but not incorporated in draft:

- Eric’s desire (but lack of actual effort) towards turning the issues/risks (first appendix) into a table that cross references those risks to approaches (noted elsewhere in the document or on the wiki) that can be used to mitigate those risks.
- Any discussion about UI issues for registering/linking new external identities.
    - On the last call we discussed that it wasn’t clear if there’s a “Right” UI to initiate the identity linking process; e.g., distinguishing between a “new identity needs to be created” vs. “here’s a new external identity to link to an existing institutional one”.

Minutes

Discussed specific edit suggestions. The ones noted on the call were:

- Remove overused instances of "e.g., ... etc"
- “Bulletize” the Architecture section; it's currently too much prose
- Need to address non-web-based applications
    - Should we call this out even when there's not a formal SP?
- What language should we use rather than “SP”
    - May need to define “SP”, “resource” or “resource provider” for purposes of this discussion
    - Possibly use the term “relying party”
- Add better notes about de-anonymization of users
    - Specific use case to discuss is how use of a shared proxy can de-anonymize targeted identifiers
    - Some discussion about whether this could be considered inappropriate by some IdPs
- Add appendix cross reference mapping issues to sections where discussed in the report
- Removed comment about possible confusion of "linking to ext id," vs. "linking to internal id using external credential"