TN - Account Linking

Use Cases

A common use case

An institution (virtual or traditional) creates a service that is designed to maximize collaboration and/or participation. The individuals participating in this service do not necessarily stay associated with any one institution over the lifetime of their participation. For example, a graduate student participating in a wiki space using an account with a strong LoA graduates and becomes a postdoc at another institution, still within the same field and expecting to remain active on this service. To bridge the use of the identity from the old institution with the identity from the new institution, the individual starts to use their Google/Facebook/other social identity account to continue to access material. Associating the old identity with the social identity and later with the new identity needs to be something the individual controls.

A set of generic use cases

Interesting Questions/Topics to Comment on.

The iPlant Collaboration wants to limit what people coming in from social identity providers can do as compared to people coming in from federated identity providers. However, iPlant, like many other VO, does not want to have to do the manual reconciliation of identity when people move from institution A to institution B. One idea, then, is to have that social identity be the bridge to link institution A's account to institutions B's account. However, having someone with limited permissions because they are coming in from a social identity provider have the power to link higher "value" federated identities... that's just not ok.

Then there's the idea that a person can link the account after they get to their new institution. But for arguments sake, one can say that they are coming from an institution that actually has a reasonable account lifecycle policy (don't laugh - this will be the norm some day) and their old account is no longer accessible in any way for linking. No authentication at both institutions simultaneously is possible. All this feeds back to manual reconciliation on the part of the VO or whoever is handling the identity linking in the service, and they don't have the resources to manage this.

Some faculty members have dual, maybe even triple appointments across multiple institutions. At Stanford University, a doctor at one of the two hospitals will have an account at one (or both) hospitals, and will automatically have an account at the School of Medicine as faculty. And, since all of this falls under the Stanford umbrella, they may well have a Stanford id as well. When they join a collaboration, the doctor/faculty member will not think about which id they signed up under, they will want all id's to have equal value and access to the same information.

UseCase 2: Institutional ID linked to Social Identity – Should Institution Allow sign on via Social Id?

- An institution creates an id locally and adds it to it's identity ecosystem.
- Said institution permits account linking (inbound, from Social Id to Institutional one)
- Should institution allow end user to sign into Social ID for regular account access?
    - Why or why not?

UseCase 3: Institutional ID (student) linked to Social Identity (parent)

- An institution creates an id locally (for a student) and adds it to it's identity ecosystem.
- Said institution permits account linking (inbound, from Social Id to Institutional one)
- Can this same scenario (UseCase2) be used to provide access to a limited number of resources using the Social Identity of the parent?
    - Why or why not?
    - The resources MAY require a higher LoA to access (e.g. student account, class schedule, etc.)

Style of linkage	Pro	Con	Comments
Inbound into institution	Ease of use for end user	password strength requirements at mercy of Social Id	This may not be the only risk