Notes-ConferenceCall-April-25-2011

notes, openid call, 4/25/2011

TOPICS -- issues around account linking
the invitation, volunteering, conscription processes for adding a person to a "group"

the call started with an informal discussion of "permanent identifiers". The attitude of US culture toward national identities was mentioned. It was noted that the Australian Federation is aleady using such a value (particularly useful in easing when a person moves from one campus to another). ORCID values were also mentioned. (although,it turns out that ORCID doesn't seem to be actually operating yet...)

short discussion about terminology -- what name should be used instead of "federated identity" to refer to campus asserted identities ? Someone asked if this discussion was really about LoA ... noted that institution affiliation is the real point in this discussion ....

CONSENSUS -- use the phrase "organizational identity".

USE CASE for using Social Identity -- using a social identity to bridge from one org account to another (eg grad student transition to postdoc)
-- want people to be able to use social identities
--- however, you would never have access to certain kinds of data if you come in from a social identity

NOTES:

-- grad student must set this up before they leave the first org
-- would we trust the first org account when they say "this social account is mine" ?
-- one you make the transition to second identifier, why not just continue using that one ?
-- org-asserted attributes may be the value add....
-- transition to social steps down the priv's within the VO (eg can no longer see budget)
why? protocol weakness (will get addressed), authN weakness.

-- especially for faculy, accounts not shut down immediately
-- and don't need to trust every social provider for the transition

-- does any campus IDM infra support account linking? ie oAuth for SAML ?
-- UW accepts linking from applicant accounts, medical providers
remote place is really acting as an RA; don't really record userid from remote place

-- does the answer depend on assessing the risk of the application in use ?
-- e-authentication developed a tool to assess risk for an SP, presented at CAMP long ago...
-- the tool itself was complicated, nebulous

stc -- implemetn linking by using ORCID ids, asserted by both org's
asserted as an attribute by both, both org's vet the ORCID id

CONSENSUS -- persisting the orig iden for six months would address this issue (except for long term unemployed)

CONSENSUS -- no clear consensus on on use of social identities to bridge

---

TOPIC -- Invitation, Volunteering, Conscription and other ways of adding members to a CO

how do individuals get a VO membership ?

https://spaces.at.internet2.edu/display/OpenID/Hybrid+Models--Chose+your+Identity+Provider+Access+that+Web+App\

https://spaces.at.internet2.edu/display/COmanage/CMP+Identity+Intake+and+CO+Enrollment\

Benn explained his flow diagrams

Scott asked about embedded registries ;
is this how apps always work? always create a new registry within their "environment" ?
if yes, there may be variations of these processes, but at the end of the day we're talking about provisioning...

Scott asked -- is there software that needs to be written to make federation doable for humans ? Are the current "user" process too difficult to use and understand ?

Benn -- in the VO context, yes, we're providing a platform
... so, are there are lessons being learned could help help apps developers whose apps will run in other contexts ?

Scott -- this process isn't unique to CO/VO, rather the general problem comes up in all federated scenarios

Steve C noted there are two categories of these applications (business -- out of band batch feeds) and collaborative (self signup, referals, invitations)