Loosely affiliated populations

name	institution	role	email
Steve Thorpe	MCNC	sys prog analyst	thorpeatmcnc.org
Tim Poe	MCNC	sr. collaborative technologist	tpoeatmcnc.org
Paul Riddle	UMBC	sr middleware architect	paulratumbc.edu
Michael Pelikan	PSU	information designer	mpp10atpsu.edu
Bradley Schwoerer	UW-Madison	middleware technologist	schwoerbatdoit.wisc.edu
Mark Scheible	NC State	iam architect	mark_scheibleatncsu.edu
Eric Buchholt	LA Tech	iam architect	eric.buchholtatoit.sola.edu
Doug Atwater	VA Tech	identity management	Dough.Atwateratvt.edu
Jason Zylks	TAMU	infrastructure services	jzylksattamu.edu
Karsten Huneycutt	UNC-Chapel Hill	idm developer	kphatunc.edu
Leo Howell	NCSU	it audit manager	leo_howellatncsu.edu
Steven Hopper	UNC-GA	it director	hoppersatnorthcarolina.edu
Liz Wendland	Duke	developer	lizatduke.edu
Dustin Slater	U Texas-Austin	idm team member	dslateratastin.utextas.edu
Rob Carter	Duke	idm architect	robatduke.edu
Mark McCahill	Duke	collaborative system architect	mccahillatduke.edu

meeting notes:

UW Madison - Federation used is to avoid credentialing everyone
why do we credential people?

- no credential at a federated party
- app that cannot use web authentication
- need to assert information to federated partners
- higher level of assurance

Can we get out of the business of credentialing some of our current audience?

What information do we really need to credential people?

Keith Hazeldon and others at UW have been look into this, see
wiki.doit.wisc.edu - search for affiliation review group

other reasons to credential:

- to establish affiliations
- to contextualize the affiliation - and an individual may have multiple affiliations/roles
  examples: professor, councilor in a summer camp, collaborator in an cross institutional research project

how does level of assurance intersect with contextualized affiliation and roles?

- should level of assurance time out?

Penn state is building a collection of registries on a fairly granular level

How do you handle multiple affiliations?

- emeritus faculty or less loosely affiliated than prospective students
- systems of record may not have places to hold loosely affiliated people
- how do you differentiate people with almost identical data (and not much of it)?

Dustin (UT Austin)

- anyone can get a credential
- never de-active netIDs
- future, current, former affiliation slots are use to manage multiple affiliations

discussion:

best effort to tie these to unique people - tied by e-mail address

federation does not solve everything - prospective students are not necessarily in a federation

UT allows for some self-identification/joining of identities (if you know the login and password)

this sort of approach is OK as long as applications do not conflate authentication with authorization
this also implies that we need to contextualize the level of assurance from the federated partners when they make assertions about individuals

OpenID or Google do not provide high level of assurance

with global campuses we will never see some of the users - but may need reasonably high levels of assurance

affiliations are groups of people and we commonly use groups for authorizations
loose affiliation implies low level of assurance - and you may not have these people in your HR system
where is the system of record for these low assurance people?

very low assurance identities typically are really just containers for preferences
3rd party e-mail is typically needed for password resets - and this may be used as an identifier
note that sometimes people share e-mail accounts though

some institutions auto-expire these loose affiliated accounts

should there be an official extremely low level of assurance to pass in addition to the gold,bronze,silver?

how do these accounts get authorized for anything interesting?

what sort of identity proofing do we do for loose affiliation?

- use case: parents using student portal system
  - parent is a "person of interest" in Peoplesoft with a birthdate
  - claim a student by naming student and student's birthday

UT remote identity proofing

- notarized signature and photo sent it or copy of passport sent in

should community document the identity vs. authorization issue?

trust issue in federations

- what does "member" mean to an institution?
- can level of assurance be tied to attributes?

some sites are using protect network identities

- concerns about connecting these IDs to institutional IDs