MACE-Dir Bof Notes of April 2007

MACE-Dir WG Meeting, April, 23 2007

notes by Keith Hazelton

-13 votes- group management in directories: practices

- James Cramton, BrownU. Import highly nested groups into Grouper, flatten. Will present on Brown Grouper in Collaboration Session on Tuesday (4:30 - 5:30, Salon K)
  Don't build apps until you have the policy; policy

- TB: Represent in ways apps know how to use: 1) isMemberOf attribute in person entry, as a group object or 2) groupOfUniqueNames or similar in flattened form in group entry

- BrendanB, USC: Affiliation-based groups and also authZ groups tied to applications "portal users;" were not doing for courses. What about courses that are sections, mapped. Are people doing this as flattened

- RL"Bob" course things are the one kind of group that we do have

- Jim Fox UDub: import automatically, flat space organized by course section, refer to by a schedule line number. Students and instructors both. clients know how to subset the population. It's accessed by clients in an LDAP directory import from DB at registrar.

- RL"Bob:" availability question: discussions with registrar. All or nothing.

- KH, U Wisconsin-Madison: Our course roster project is bringing together custodians and consumers

- JC: Registrar: This is the official list; we sometimes need the vagabonds...official + others; three effective lists per course;

- MRG: Shouldn't we get the registrar to handle the "vagabonds?"

- Klara Jelinkova, Duke: we call them affiliates; e.g. photography course with outside students. How can we reuse the current biz process to incorporate this. How does the biz process flow so that whatever groups are being created, they have to be reflected into the authoritative systems

- TBarton: Structural considerations: mission collision: "Please, registrar, do this which extends beyond your traditional mission for the good of all." This is one example of what delegated authority is about. IT can't be the authoritative system. Authority is shared in some cases.

- JP Robinson, UAB: It's a scoping issue. Professor is authoritative for some decisions, does it need to flow all the way back to the registrar's data stores?

- SCantor, OSU: We treat course related info as mostly a provisioning vs. a group problem. We find you never want to automatically de-provision. When student drops a course, no one wants them dropped 'cause they're often about to re-register for a different section. We don't have apps going off to see of person X is in group Y.

- MRG: Many see group management as an aid to provisioning...Lots of us have group-enabled applications where the group object in the directory is a first class service

- KJ: We have some apps that simply say, if this person is in the directory, they're authorized for my app.

- David Walker, UCOP: Provisioning is a workflow, so issues of timing play a big role. If AuthZ is implied by membership in a group, membership (or not) shouldn't be the sole basis for access to services.

- Jim Fox: many thousands of groups;

- Keith: Lifecycle, state machines, grace periods.

- JC: IT group is stuck between rock & hard place: Registrar and HR are 20-30 year old systems. Historically we have user group needs that are "met in other ways. IT is in the middle. We are more agile than the registrar, more production than the quick one-offs

- TomD: Our registrar's system is old enough to be drafted. IT is authoritative for more and more over time, it makes us nervous, but what are the alternatives.

- JPRobinson: It may be justified to have many authoritative systems.

- TD: CS department has their own IdM infrastructure. They and others flatten these intrinsically hierarchical, nested groups for internal use.

- Heather Flanigan: StanfordU. SHameless!!

- Scotty Logan: Stanford: Rich notion of affiliation subtypes and roll-ups.

- RL"Bob:" Discussions have commenced on chartered activitiy to when we were defining ePAffiliations, they were a carefully controlled set. There is pressure to increase. Specifically for those with library privileges. The info in the current spec defining faculty and staff is minimal, could be better. Notion exists that the entire set of definitions could be made more precise. Students off for a term student or not, adjunct faculty faculty or not. Qualified affiliations: student:onLeave. Recently at Terena: The affiliation values need to be multilingual

All vs. ePEntitlement

- Kathryn Huxtable, KU: we made our own KUeduPerson. MACE-Dir could help by capturing some good/best practices, but should not actually get into defining values for local use. Even for eduPerson level.

- TB: library privileges question. Are there other specific use cases that would drive us toward a workable problem set?

- RL"Bob:" Let's define things that seem useful and see what happens. Student affiliation in particular is likely to be generally useful because resource providers are looking for ease of use and are not particularly concerned about precision of definition (some leakage ok).

-MGrady- We say that survey staff are library entitled, but are not faculty staff

-Etan, Johns Hopkins: Throw specifics over to the entitlement side. Should ePA values be informational only? At Hopkins, we were never sticking to the controlled vocabulary for ePA.

-Thomas Lenggenhager, SWITCH: ePaffiliation is good enough for deciding access questions. Internally, that's not enough.

- TB: TL was giving what a value meant in a specific application context. More generally we need to have the discussion IN CONTEXTs. We will benefit from this pragmatic stance.

- KHuxtable: Our library signs contracts that we will provide access to campus X but not campus Y. In practice we do our own authZ and it's accepted. EZProxy handles the details. I don't see third-party vendors using that type of information...Student isn't useful at a single institution.

-BBellina: ePA is good as a discussion starter. It's a use at your own risk since there are not published definitions anywhere. It would be safer to release entitlements.

-RL"Bob:" It's all risk management. On the other hand: if every conversation with app. providers starts with there are entitlements, let's consider the entirety of the entitlement space. If we can get some mileage with ePA, then we're better off. We can't afford the endless conversations that would ensue without ePA.

-MRG: we need the discussion about whether an existing attribute/values will work, whether we need something new....

-RL"Bob:" resource providers have 10s of thousands of contracts, so if you propose to solve this, you have to have a solution that will work for ALL the places.

-Scotty L: Roll-ups to ePA. We can do affiliation math in the Attribute Release Policy.

-TBarton: some practices may differ on campuses, but that doesn't mean more global solutions are completely invalid

-ScottyL: We have visibility flag on each attribute in our Enterprise Directory

-8 votes- philosophies of dirs, ws, saml,

-MRG: Shifting to the philosophy question: Directories vs. databases vs. attribute authorities vs. SAML...

-ScottyL: webAuth, webAuth with LDAP; guest users separate system, so now we have to go with Shib. Course info is NOT in our directory (funding issue). We have to go with SAKAI.SAKAI can be behind a Shibboleth Attribute Authority.

-SCantor: The decisions come if you don't have X in place today, do I need to build it, or is it more effort than it's worth. Difference between what you run internally vs. what you expose to applications. You want to insulate apps and app code from changes in IdM infrastructure. Anything else is really dangerous.

-MRG: what about apps that require something you don't have?

-SCant: That app is broken. We don't have $ to fund new customized solutions.

-BBellina: LDAP does things I like, I have concerns about non-LDAP solutions. Shib doesn't solve problem about access to OTHER people's information; web services have some buzz, is another smart layer, where does the intelligence go?

-SCant: Gain something, cost of complexity: Get info on others, but different info in different contexts can also be supported. Real-time, presence-oriented

-Roland Hedberg, UMEA: We've been pointing apps to web services rather than LDAP so we can put logic in the exchange. Don't want to show all the values for any particular attribute.

- SCant: We're basically working on things that fill gaps that LDAP hasn't chosen to handle. WS (incl. SAML) are more in flux, still. Maybe we'll get to a point where WS's no longer are flexible, are "mature," stable and resistant to change. Then something else will have to address need for agility.

-MRG: Would you do WS for mail routing??

-Roland: We're using WS for lots of things; LDAP for the things that know about LDAP and have simple needs; Problems come with new apps where developers don't know what LDAP has and what it can do, and they push the envelope. We're going to provision in those cases because it would break the LDAP directory.

-ScottyL: Aggregation layers: pick the layer in the stack that's appropriate

-5 votes- MACE I2MI attribute profiles for SAML

SCant: message sent to list last night. Product interoperability problems and software constraints we're working under; strawman solutions

-KJK: UK: requirements: no reassignment of ePPN, ePTargetdID for two years.

-SCant: ePTargetedID doesn't make sense to be reused ever. Maybe we need to revisit that.

-Rob Banz, UMBC: When I did ePPN, I put in esssentially Kerberos principal; With shib, I wanted to switch to an opaque identifier

-RL"Bob:" There were considerations of human friendliness, handleability with ePPN.

Topics for future discussion

3 votes - the directory wars
2 votes - ePAffiliation, ePEntitlement values
1 votes - ePAccount
1 vote - application integration
0 votes - patron