COmanage Call 3-Mar-2011

COmanage-dev Call 4-Mar-2011

Attending

Heather Flanagan, Internet2 (chair)
Ken Klingenstein, Internet2
R.L. "Bob" Morgan, U. Washington
Keith Hazelton, U. Wisc
Steven Carmody, Brown
Tom Barton, U. Chicago
Jim Leous, Pennsylvania State U.
Benn Oshrin, Internet2
Steve Olshansky, Internet2
Emily Eisbruch, Internet2 (scribe)

New Action Items

[AI] (Keith) will make sure that the COmanage glossary covers roles and groups accurately. https://spaces.at.internet2.edu/display/COmanage/Glossary

[AI] (Ken) will provide a link to the French listing regarding applications and sets/bundles of attributes.

Carry Over Action Items

[AI] (Keith) will add to the COmanage wiki use case library the case of bridging identity using social identity credentials.

[AI] (Keith) will ask Roland and Leif to clarify how social identity assertions will be handled in their system.

[AI] (Benn) will update the COmanage roadmap based on recent discussions with COs.

[AI] (Benn and Keith) will talk about Bamboo's requirements for person registry.

[AI] (Ken) will contact David Groep about VOMS GUMS.

[AI] (Steven) will develop a one-page write-up on attribute aggregation.

[AI] (Heather) will ask U. Chicago people to contribute an academic (intra-institutional) use case to the COmanage use case library.

DISCUSSION

Groups and Roles in CO Context

Comments included:

Definitions:

- A group is a collection of things.
- Roles – a set of duties that go with a position

StevenC: In a permission system, groups are one of the things that can get mapped to roles

A position (job title) can also get mapped to a role

Benn: the COmanage development effort does not currently include the objective of doing something with roles. We need requirements before we deal with roles.
TomB: Grouper incorporates the NIST RBAC model http://csrc.nist.gov/groups/SNS/rbac/

RBAC includes notions of role hierarchy and inheritance

[AI] (Keith) will make sure that the COmanage glossary covers roles and groups accurately.

https://spaces.at.internet2.edu/display/COmanage/Glossary

Status Update (Benn)

- Benn has added new items to COmanage JIRA https://bugs.internet2.edu/jira/browse/CO
- A lot of the JIRA items resulted from the recent conversations with LIGO
- Code is in SVN -- there is an anonymous SVN and an authenticated access SVN
- The anonymous SVN may lag behind the authenticated SVN
- The code corresponds to the demo running on Benn’s laptop

- Will move the COmanage demo to the Internet2 servers soon
- Benn is currently working on COmanage Gears (profile management)
- Focus is on getting institutional identity and correlating that with the CO identity.

Q: Keith: Does COmanage Gears currently rely on some implementation of registry and/or Grouper?

A: Benn: There are no external dependencies except for framework (php). On the roadmap: insert the FIFER group API and connect that API with Grouper https://wiki.jasig.org/display/FIFER/Group+API+Data+Structures+and+Operations

Social Identity

Question: Is what VOs need in the social identity area simpler or different from what brick and mortar institutions need?

Jim: it depends. At Penn State, we are bricks and mortar but spread over 24 location but we have a strong central identity, so can organize Penn State VOs without Shib. But at other institutions, it's possible that they need Shib to make the institution more amenable to cross-unit collaborations

StevenC stated that there are three categories of use cases driving the social identity discussion:

1. Institutional applications where the owners want to accept social identities. An example is CMU using social identities for access to student bills. Parents won't have SAML identity, so parents will be able to use social identity to view the student bills.

2. VOs who want to use social identity because SAML has not fully taken off in the U.S. People want more people accessing their site. Examples include VOs funded by NSF and smaller, more ad hoc collaborations.

3. People who are experimenting, sort of playing with social identity.

Jim raised the example of DISQUS, used by newspapers and online blogs... where a user can access the discussion using their social ID. The user can then go on after using their twitter identity to set up an account and can add things that don't exist in their twitter account. http://disqus.com/

Push Vs Pull Issue Raised on International Collab Call of 3-March-2011

- There was discussion on the International Collab call of different collab management platforms
- Leif said Comaange is a push platform, whereas other models are pulling info
- This is set on the background of the Blakely article and idea that the future is pull, http://mms.businesswire.com/bwapps/mediaserver/ViewMedia?mgid=237020&vid=1
- There may be some perception of traditional Enterprise IdM where there is a central repository of info that gets pushed out to other systems that the central enterprise can thereby control.
- This perception is connected to central planning (push) and free market (pull)
- There are not currently apps that support the pull model, so it's hard to imagine it working in the near future
- An alternative for IdM folks is to offer an open service, but not sure how that relates to the VO scenarios
- Leif was talking about applications that can dynamically generate a query during processing. A kind of late binding, not something that happens at logon time. No applications do that today.

What we do see now in attribute aggregation is this scenario (Steven has a working demo for GENI that does this):

- I have a campus ID and I am a member of VO1
- VO1 has a portal, that serves as a front end for a device I can use.
- I login to the portal, using my campus ID,
- The portal is configured to query VO1
- VO1 provides info about my permissions.
- The portal agregrates what the campus provided and what VO1 provided
- That can be called reputation building.
- Steven noted that in case of GENI work, we might spit out x509 certificates into GENI space from COmanage, so there will be a single root for the commands coming into the apps from COmanage.

But is having COmanage as a broker going to simplify the trust process for the application?

Steven: GENI and the grid are two of the spaces that are wedded to x509. They fit into the federated framework where SAML2 metadata provides the trust. There is heavy reliance on PKI.

There are use casees these days where people want a more dynamic situation, where it could be possible to instantly stand up some service and people would learn about it and trust it.

A lot of apps these days, people can find ways to wrap SAML and its metadata - based trust fabric around it.

Q: What about CI logon?

A: CI logon works for the grid because there is a well-defined trust infrastructure on either side for mapping. There is login w SAML identity. It leverages SAML2 metadata to establish trust. CI logon has two CAs operated in proper fashion.

CI Logon may be used in other spaces, such as OOI. Talking with GENI too.

Attribute Bundles

JimL: The CIC IAM group is discussing attribute bundles, and will possibly promote that to rest of InCommon.

There is also talk about this within VIVO http://www.ctsi.ufl.edu/2010/05/01/vivo-enabling-national-networking-of-scientists/

Ken: The French are working on categorization of applications and developing sets (bundles) of attributes. The idea is that there are natural categories of applications where it makes sense to recommend a particular attribute bundle

[AI] Ken will provide a link to the French listing regarding applications and sets/bundles of attributes

Keith noted that U-Wisc has an attribute bundle project.

Steven: InCommon operations hopes by April to allow SPs to add requested attribute elements to their federation metadata.

Next COmanage-dev Call: 18-March-2011