COmanage Face-to-Face Meeting 5-Oct-09 and 7-Oct-09

COmanage Working Group Face-to-Face Meetings
2009 Internet2 Fall Member Meeting in San Antonio
5-Oct-09 and 7-Oct-09

5-Oct-09 COmanage Working Group Discussion

*Background on COmanage as a Service

Heather provided an overview of COmanage project developments. Two years ago a demo COmanage product had been shown. Then the COmanage development team turned to creating a COmanage appliance. This turned into a system administration exercise more than an identity management exercise, and it became apparent that system administration was not the correct focus. In the past few months, there has been a return to working on the demo COmanage version, with the focus on COmanage as a service to collaborative organizations. Michael Gettes has brought the live COmanage demo up to date and integrated new applications.

Questions for discussion:

- Who will provide the services for this service model?
- How should it look in the future?

Demo

MichaelG presented a demonstration of the service COmanage demo (co.internet2.edu)

Features:
- Gives control to community members
- Flexible, scalable, modular
- Shibboleth infrastructure is used
- Grouper is used for management of groups, hope to incorporate new Lite Grouper UI when available in the forthcoming v1.5 release (with fuller Grouper UI still available for the collabmin)
- Includes WAYF, courtesy of SWITCH
- Provides applications, such as Confluence, calendaring with Bedework, web conferencing with OpenMeetings, mailing lists with SYMPA
- Includes forums
- COLLABMIN tab allows for administration, such as viewing permissions
- Ldappc runs in the background. Updates every 60 seconds. Ideally, it should instantly provision upon an event happening.
- Some documentation still remains to be done.

COmanage uses the UID and eduPerson information supplied by the identity provider. Applications that don't allow an @ sign are a problem. Bedework didn't used to be able to handle the @, but now it can. It could be possible to use a mapping capability to work around such @ sign problems.

Q: What about the difference between self-assertions and verified assertions?

A: This can vary by CO. One CO could disallow the user from changing his own email address, while another CO could allow this.
Heather noted that the international component of collaboration management efforts has been interesting. Hope to get more discussion on that in the second COmanage session at this member meeting.

Leif stated that one thing missing is the ability to associate attributes with something less permanent than a directory entry. The attributes in the directory from a federated source are permanent.

In the GN2 JRA5 project, various approaches, including LDAP and OAuth, are being looked at. OAuth may offer a less permanent association with attributes and an easier way of doing entitlement management.

R.L. "Bob" mentioned the "user-managed access" approach of authorizing a linkage between SPs via an IdP acting as an access manager; people are building this based on OAuth.
MichaelG commented that there are interesting challenges and the approach is to do something real that can be realized now. A lot of apps know how to do LDAP, and most likely in future, a lot will know how to do OAuth.

Leif: not all apps fall into same box concerning attribute delivery. It's important to keep these things in mind so COmanage doesn't go away when LDAP goes out of style.

COmanage and Google

Steven raised the question of the advantage of the COmanage approach vs Google apps. Answers included:

- Google doesn't get to mine all your data in the COmanage approach
- Local authentication that binds back to the institution (though if you want people to still access the apps after they've left your institution this - can be a disadvantage)
- Better security
- Access management options in COmanage (granular authorization on user base)
- Google apps has problems handling interdomain usage. Could be solved in the future.
- Range of apps offered could be wider with COmanage

Next Steps

There was a discussion of the degree to which the COmanage identity should be apparent versus just have users see the applications. Perhaps use a customizable "splash page."

MichaelG hopes to get Foodle scheduling software integrated into COmanage. Needs simple SAML to work with InCommon. There is some work going on in Europe that could smooth the way.

7-Oct-09 COmanage Working Group Discussion

Ken noted that there will be several versions of collaboration management platforms developed in different places. What are the touch points? What do we need to do somewhat consistently? What can we do independently?

There may be a touch point around applications and what we want to ask them to do. MichaelG noted that he had had productive conversations with the Sympa developers and there were plans to work together more in the future.

Projects can share information on integration of applications: e.g. OpenMeetings is relatively easy to integrate, Drupal is more challenging. There are different degrees of domestication.
Consistency in look and feel of different collaboration platforms being developed is not important at this time.

It was agreed that this conversation should continue on the Collaboration calls. The suggestion was made that we can use a COmanage instance to coordinate these discussions.

There was discussion of restructuring the COmanage email lists. More to come on this as it develops.

Neil W. described an Australian use case. They have several services, Drupal, etc. and need a way to manage authorization rights to those services. They were considering building access services for registration and access rights. But questions arise concerning changing attributes. It was agreed that sometimes an IdP is needed on top of the CO. Putting an IdP bundled in front of COmanage was in an initial plan but has not been tackled yet.
An upcoming release of Shibboleth SP will allow a higher ed institution to push a bundle of attributes to application with a pointer to where to get more attribute info.

PaulH has had discussions with the OpenWebware community. They have many wiki instances around the world, and different collaborators have different accesses. They became their own OpenID identity provider. They use Facebook as one of their tools and they'd like to pull data out of Facebook when people are logged in. But the OpenWebware community wants to get closer to University way of doing things. They had issues with data being stolen.

Three deliverables:

1. Keep the demo site up to date, use it for collaboration calls
2. Create a "recipe" , documentation for people in the technical aspects of this environment
3. Work on domestication of more applications or giving feedback to more developers on providing the external info