COmanage Call 18-Mar-2011

COmanage-dev Call 18-Mar-2011

Attending

Ken Klingenstein, Internet2 (stand-in chair)
RL Bob Morgan, U. Washington
Keith Hazelton, U. Wisc
Ann West, Internet2
Dan Pritts, Internet2
Steve Olshansky, Internet2
Emily Eisbruch, Internet2 (scribe)

Carry Over 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.

[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

VMs

Danno has inquired recently on the list about the status of these VMs on the Amazon cloud:

comanagedemo.internet2.edu
comanagedemo2.internet2.edu

So far no one claimed ownership. SteveO will email Chris Hubing about them (DONE).

VO CAMP

- Ken has been in communication with the NSF about the VO CAMP.
- Most likely timeframe is September 2011 or later.

COmanage Demo

- Ken has been testing the COmanage demo (which is now on a VM) and working on a demo flow in relation to the GENI work.
- Benn has been responding to any issues that are identified.
- There is a call scheduled for Tuesday, March 22 for Heather to familiarize the Bamboo team with the COmanage demo.
- Ken stated that the only people listed on the demo instance are people Ken has added for his GENI demo
- Question of whether Keith can use those same people for his Bamboo-related demo workflow.

Ken explained the flow in his demo so far:

- Creating a new VO on the demo instance
- inviting people to join
- Creating a group within the new VO (Note that there are some screens that need work)
- Keith plans to do the Bamboo equivalent of that and hopes to go farther based on what Bamboo researchers want to do (like access repositories of texts, etc.)

- Ken noted that COmanage versioning was recently incremented.

COmanage Team

- Ken plans to have some discussions with Heather and Benn concerning software development and sustainability
- Want to be sure that we have enough depth / coverage on the team
- It was noted that using JIRA and SVN -- as Benn has been doing --- is important

GENI Update

- Ken recently attended the 10th GENI Engineering Conference in Puerto Rico http://www.geni.net/?p=1984

- GENI will join InCommon, and they plan to use federated logins on their portal
- Most likely GENI will join InCommon in this new category http://www.incommon.org/fees_research.html

The PKI Backend

- The GENI use cases may require construction of a non-SAML, non-LDAP delivery mechanism from COmanage.
- This might be a table-driven x.509 delivery mechanism where construction of certificates is determined by the target.
- Jim Basney might work on this.
- One of the GENI use cases apparently gets x.509 certs from people, then collects data and assigns privileges based on a form with self-asserted attributes that do not get added to a certificate.
- People Ken spoke with associated with Attribute-Based Access Control (ABAC) remarked that if COmanage could produce attributes that would be great
- QUESTION: Do we know of use cases (apart from GENI) that require a x.509 backend?
- Keith remarked that work at University of Kent could be related

Terminology

- Is there a word to describe the mechanism for moving attributes from COmanage instance to an application?
- What is needed is an umbrella term for exchange of SAML assertions, for apps make LDAP calls, and for other kinds of provisioning
    - Connector ?
    - Backend ?
    - Vehicle ?

DECISION: Use the term Attribute Delivery

COmanage and GENI

GENI program office (GPO) does not have SSO across their applications, nor does BBN Technologies
There is no enterprise directory, however there are hundreds of graduate students participating in the GENI projects, needing access to resources
Ken talked with GENI about the advantages for GENI personnel to be able to use their login to access resources.

Would it make sense for GENI to have two COmanage instances:

1. COmanage inside the GENI portal , as a place where various researchers would manage permissions and capabilities for their students and other researchers' students.

and

2. Could there be a COmanage instance inside the GENI Project Office (GPO) functioning as a pseudo enterprise directory? This would involve embedding COmanage in the GENI management portal. All the attributes would be self asserted.

RL "Bob" remarked that every organization can benefit from a COmanage instance as long as

- They are prepared to run it and
- They have apps that can use it and
- COmanage is at a proper stage of readiness

Ken: Summer timeframe for having set this up within GENI.

Ken raised a question about defining permissions to class members. Assume I create a class using GENI and all individuals in the class have the same sets of permissions. Would it look like a single group entry in COmanage? So that when you get to the portal you map to the group. and get the permissions from COmanage? OR would every individual in the class need their own entry in the COmanage person registry?

Steven had indicated in the past that it would most likely be possible to put groups inside the person registry

Ken saw a recent email discussing this (PG PR registry ?) Ken will send that email to the list if possible.

RL "Bob" : Perhaps the question is whether there is justification for COmanage to be an IdM on its own with its own UI etc. ? Or should it just be the set of functionality embedded in something like Drupal

Keith observed that with Grouper, both delivery approaches were used. Grouper was delivered with an admin UI. Then Grouper was delivered with web services to accomplish most of the Grouper functionality. That's the model -- get something useful out there (so need to develop some UI screens). Then pitch the idea to others to call functions from Grouper.

InCommon News

There is a new membership category in InCommon for research groups. http://www.incommon.org/fees_research.html

There is endorsement on steering committee for bringing VOs in.

LIGO and GENI will both be joining InCommon in this category.

Trust Issues

Managing trust routes in GENI is challenging. Currently, accepting credentials from other clusters is problematic. They want a coordinated infrastructure.

Does using a PKI attribute delivery mechanism simplify matters because they just can trust COmanage and Comanage will then deal with federation and metadata? Does it make sense to simplify trust at the PKI level by making Comanage the only CA that the various clusters need to know about?

Ken: Is there parameterization that COmanage needs to go thru? A COmanage instance in InCommon needs to ingest the InCommon metadata. Is it doing that today?

The COmanage demo has something called organizations. These provide identity.

Keith will ask Benno what is behind the organization field at the 22-Mar-2011 COmanage/Bamboo demo intro session.

The evolution of metadata has put InCommon and the Shib and SAML folks ahead of many federated organizations in terms of managing trust in scalable ways

Bob re boarding process. if COmanage is an SP, accepting identities from IDPs, it would rely on its SAML software (Shibboleth) to do SAML processing of metadata. But how does it manage the IDPs that it is working with and their metadata? That could be a piece of application requirement we do not yet have standard functionality for.

Ken: What about a listing of the various IdPs that could work for a particular COmanage instance?

RL Bob: This listing is found in the discovery service that is embedded in the app. The way to find out if your organization is able to use an app, is to go to that app and looking at the list that pops up. There most likely is a requirement for exposing that for other purposes. This is part of dealing with the boarding process and making it easier.

Dyonisius posted some interesting information on this on the MACE-Dir list on 3-Dec-2010.

VO Updates

- **iPlant**
- iPlant is contracting with the IRODS people to create a Shib'ed version of IRods
- IRods talks about micro policy
- It's still unclear where we link into IRods with permissions -- discussions are ongoing

- **Federated SSH**
- Things are going well with the Federated SSH project. Sam and Josh will be presenting Project Moonshot at 2011 SMM.http://events.internet2.edu/2011/spring-mm/agenda.cfm?go=session&id=10001724&event=1035
- The hope is to get federated SSH clients into people's hands
- Keith: Could be positive for someone involved in Federated SSH to join a MACE- paccman call; this could be a use case for the policy issues MACE-paccman is looking at.

2011 Spring Member Meeting in Arlington, VA

_____

COmanage Working Group at SMM:
Monday, April 18, 2011, 9:15 AM - 10:15 AM
Location: Salon A
http://events.internet2.edu/2011/spring-mm/agenda.cfm?go=session&id=10001750&event=1035

_____

ALSO AT SMM:

International Collaboration Platforms – SURFconext, COIP, COmanage

Monday, April 18, 2011, 4:30 PM - 5:30 PM

Location: Salon D/Ehttp://events.internet2.edu/2011/spring-mm/agenda.cfm?go=session&id=10001706&event=1035

Supporting Research Communities: Collaborations in Action

Tuesday, April 19, 2011, 1:15 PM - 2:30 PM
Location: Salon I/II/III http://events.internet2.edu/2011/spring-mm/agenda.cfm?go=session&id=10001705&event=1035

Next COmanage-dev Call: 1-April-2011