COmanage Call 20-Jan-2012

Minutes: COmanage-TAC call 20-Jan-2012

Attending

Heather Flanagan, Internet2 (Chair)
Ken Klingenstein, Internet2
Keith Hazelton, University of Wisconsin - Madison
Scott Koranda, U. Wisconsin - Milwaukee (LIGO)
Steve Olshansky, Internet2
Emily Eisbruch, Internet2, scribe

****Carry Over Action Items***

[AI] (Heather) will set up meetings with IRODS/iPlant/Internet2 in February

[AI] (Keith) will check whether the Project Bamboo IAM infrastructure work plan is available on the wiki, and if yes, he will send the group a link. (DONE)

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

DISCUSSION

Policy Decision Points
   - in the app or in the platform? what should be the criteria?

Ken:
- Policy Decision Point question has come up in terms of IRODS domestication
- When should the PDP app versus in platform?
- IRODS has a very rich policy environment, they use XACML, use micro policies
- But is this is a capability that we need?
- For VO instances, perhaps it's generally sufficient to use simple policy mechanism based around a priv or role you have in the VO
- Where we pass in "this person is permitted to do it " and "this person is not"
- Will there be a guidance we can offer VOs for when to put the PDP inside the application versus outside?

Keith :
- very interesting from the MACE-paccman point of view
- most orgs find that SAML does most of what is needed, XACML solution is not needed

Ken:
- IRODs mentioned that after authentication, they'd like to use a script to provision an account
- this could be a unique approach, using provisioning
- could be a chance for SCIM or SPML mechanism?
- our goal is to help IRODS build a prototype domesticated app

- ScottK noted that PDP is part of the LIGO picture
- For an application that is fresh and LIGO has control over it, it's easiest to do the work inside the app
- this is because the infrastructure for external handling is not yet in place, so easier to write quick code
- but there are many legacy apps that need to be retrofitted
- would be good to have an external management of permissions

- specific example is the Document Control Center
- people are asking for more and more access controls
- hard to retrofit
- offering a better way would be attractive to LIGO

- ScottK: there is now a citizenship committee looking at "dual citizenship" issues (folks in two collaborations)

- Ken: wonder if a group management solution with richness of access control could work?
- Ken: would be good to have a document to guide decisions in this area
- Heather: how do we get enough guidance on this to write a helpful doc?
- Ken: we need a paragraph to frame the question
- AUTHZ is something we want to manage with efficiency
- over next months we will be looking at use cases and trying to make generalizations
- then Keith could take that to MACE-paccman

- Keith: the Project Bamboo planning work has taken the policy issues seriously
- at the conceptual level, the Bamboo system is designed for using a policy engine

VAMP

Ken:
- NSF is highly supportive of VAMP (VO CAMP)
- NSF is ready to receive a SAVI grant on this that Ken is developing
- Could be early Sept. timeframe (Ken is consulting with Europeans on dates)
- Have started a list of key VOs, including:
    - LIGO, IPLANT and Elixir-Europe
    http://www.bbsrc.ac.uk/science/international/elixir.aspx
    - Project Bamboo and Clarin
    http://www.clarin.eu/external/

Scholarly Identity

Ken:
- Scholarly identity was discussed on recent MACE call
- InCommon is focusing on this area
- Scholarly identity will be a policy discussion at CSG in June in IOWA
- A recent Cliff Lynch podcast touched on Scholarly identity issues

- Keith noted that Dedre and Lucas are working on account linking issues
- Ken noted there are issues around account linking: LOA and unidirectional verus bidirectional

COmanage and Externally Hosted Services

- People are enthusiastic about the progression of Foodle and the opportunities
- The Dutch may be be planning to use the Norwegian service instance of Foodle (possibly using Voot?)
- Could it ever make sense for COmanage to run an external instance of an application, such as Foodle
- What are the issues around this?
- Could be too early to tackle this.
- But Ken may talk to Andreas about this and will keep this group informed

SMM 2012

- Heather: we will be thinking about sessions to put on agenda for the 2012 SMM in April
- It was noted that number of timeslots for Middleware sessions will be more constrained than in the past
- Middleware and InCommon are part of the Net+ "area of interest" and many of the slots may be taken up by new Net+ services.
- But COmanage could potentially be part of another area of interesthttp://events.internet2.edu/2012/spring-mm/calls-proposals.cfm

Next Call: Friday, Feb. 3 at 2pm ET