

CManage Call 7-Jan-2011

CManage Call 7-Jan-2011

Attending

Ken Klingenstein, Internet2 (stand in chair)
Keith Hazelton, U. Wisc.
Steven Carmody, Brown U.
Chris Hubing, Penn State
Benn Oshrin, Internet2
Ann West, Internet2
Dan Pritts, Internet2
Steve Olshansky, Internet2
Emily Eisbruch, Internet2 (scribe)

New Action Items

[AI] (Ken) will develop a one-page writeup on the differences between a VO IdMS versus an enterprise IdMS

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

[AI] (Ken) will email Bob B. regarding the possibility of speaking at ACAMP

Carry Over Action Items

[AI] (Heather) will include a discussion of a 3rd CManage VO as topic for the Tuesday call. (DONE)

[AI] (Heather) will schedule an Internet Identity webinar for iPlant IT staff.

[AI] (Heather) will arrange a meeting with iPlant in Tucson. (DONE)

[AI] (Heather) will add questions about role transition to the assessment document. (DONE)

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

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

[AI] (Jim) will check on whether there has been discussion on the CIC list concerning LIGO and the domesticated apps list.

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

[AI] (Jim) will share ESWN call notes with the CManage-dev list.

Discussion

Registry

Registries were discussed on the 3-Jan-2011 MACE call.

Geant3 has a Namespace registry, which is essentially a service registry. <http://www.geant.net/Services/NamespacesRegistry/Pages/urngeantRegistry.aspx>

CManage is focusing on person registries in the VO context.

It was noted that issues around service registry versus person registry are different, but there is overlap regarding identifiers and accounts. Service registries must authenticate to each other.

Could the VO registry work being developed in CManage could be applicable to the enterprise registry space?

Benn: It would be helpful to define what we mean by the word registry, especially in the person registry context. What are the boundaries of a registry? When is it an IdMS?

Keith: Definitions of registry have been discussed in MACE. Registry involves aggregating multiple sources of Identity info into a single place. Sometimes this involves identity reconciliation. On the outbound side, registry involves a point of access to authoritative info., not the source of authoritative info.

Q for Benn: As you develop interfaces to handle automation of business process for LIGO, does it turn out to be library of routines that people use? Will these be portable? What is relationship between encoding of business processes and the registry?

Benn: We are working with LIGO on workflows for the enrollment processes, and the flip side is the expiration processes. There seems to be a relatively constrained functionality to implement for LIGO. Within CManage, it will likely be a few customizable web pages. Initially it may need programming skill to get it up and running. Longer term possibly it will all configurable from an XML file or some thing clickable.

Ken: Are those components – enrollment and expiration processes – sharable across implementations?

Benn: In the short term, programming skills are needed, in the long term, this functionality will likely ship as part of the CManage product and will need some on-site configuration.

Keith: There are two important aspects, and the CManage work is a combination of those two things:

- 1) Setting up an authoritative source of person info. We generally think of the registry as downstream system from those authoritative sources.
- 2) Exposing those sources in consumable ways to things downstream from it

It was noted there are also concerns about ensuring there won't be more than one source of data about people.

Benn stated that there are other agendas related to registries, such as open registry design, and the classic enterprise model, with upstream systems of record. In the CManage model, the upstream system of records equates to external institutions. The person registry within CManage would need to provide system of record functionality as well.

In the case of LIGO it's the upstream schools that provide its members that represent the SOR.

Keith: U Wisc is writing a module to handle the "other" (external SOR) category for its group and affiliate management service. This service is based on Grouper, but there is a need for a way to handle outside people. (This may be handled by Grouper 2.0.)

Keith advocates treating the SOR as a separate module within CManage. If CManage was designed in a modular fashion, then U-Wisc could leverage that SOR module.

Steven: There may be a need for a credential service. Some folks authenticate by openID, but in some cases there is a need a higher LOA. Some people don't have access to authentication that could provide that higher LOA. What about interfaces between the LIGO Kerberos instance and CManage? Some VOs will need to issue a small number of credentials associated with local accounts.

Benn: Yes, this is where CManage starts to move up a notch or two towards the Enterprise IdMS. We had expected to have provisioning on the backend, but now that will include account management infrastructure to manage the Kerberos realm. On front end, whether you get data from another SOR or from storing it in CManage directly, it will be a customizable plug and play.

AI (Ken) will develop a one-page writeup on the differences between a VO IdMS versus an enterprise IdMS

Steven and Keith predicted that the difference will be in the ratios of people from various sources. Both the VO IdMS and the enterprise IdMS will have to manage people from various sources

Registry issues will be discussed at Internet2 2011 SMM, either in a track session or a BoF.

Keith expressed enthusiasm about the upcoming release of Grouper 2.0 and its support for external users/ members of groups. This release will address issues U-Wisc is facing.

It was noted that the person registry activity is important not only to LIGO, but also to other organizations involved with CManage: iPLANT, ESWN, ICERN and Bamboo.

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

Blakley Article on Push Versus Pull

Ken recommended reading the Gartner article on "The Emerging Architecture of Identity Management." This article can be accessed here:

<http://mms.businesswire.com/bwapps/mediaserver/ViewMedia?mgid=237020&vid=1>

Keith stated that the article will be discussed on the 20-Jan-2011 MACE-paccman call.

Keith and Steven agreed that the article is forward-looking, and the transition to pull will be a slow process. For example, Brown is replacing engines in its IDM system and one of the goals is to move from overnight feeds that push to real time push. Brown is not alone in focusing on push. Many institutions will not do pull for some time.

Ken remarked that there is an emphasis on push in the national provisioning project deployed in Denmark.

Updates from Project Bamboo

Keith reported there is an effort to pick up the momentum in Project Bamboo..

There is movement on workspace and IAM issues and a plan to start coding for the 1st round of deliverables.

HubZero may be the portal for Project Bamboo, at least in the demo stage.

Update on Dutch Collaboration Platform

The Dutch have put the COIN infrastructure into production at beta sites.

There is work at Oxford around Project Bamboo. Neils will provide us with a contact name.

SURFnet was approached by Apache, regarding another portal built on OpenSocial

COIN plans to give users control over attribute release. Benn noted we are still too early in the CManage project to address issues of attribute release control for users

Update on ESWN

Steven reported that ESWN has started implementation work. ChrisH at Penn State is wiring up Shib under the Drupal interface.

Chris is working on an OpenID login at Penn State. It will make sense to port that over to ESWN.

Steven hopes to have an ESWN CManage demo available at 2011 SMM

Update on iPlant

There is an upcoming iPlant meeting in Tucson to gather requirements and plan. iPlant has some different requirements from LIGO. That is good for the overall strength of the CManage product. ScottK of LIGO will come to the iPlant meeting. Cooperating VOs is a positive.

Upcoming Meetings of interest

Internet2 Spring Member Meeting <http://events.internet2.edu/2011/spring-mm/>

TomB is coordinating a team working on the two tracks covering our landscape: Middleware Track and Focus on Federations Track

Jasig's Spotlight on Open Source, May 23-25 in Colorado <http://www.jasig.org/jasigs-spotlight-open-source>

Advance CAMP: Identity Services Summit - May 25-27 in Colorado

AI (Ken) will email Bob B. regarding the possibility of speaking at ACAMP

VAMP (VO CAMP) we are waiting to hear about funding

IDTrust 2011 <http://middleware.internet2.edu/idtrust/2011/>

Next Call: Friday, 21-Jan-2011 at 2 pm ET