Advanced CAMP Notes

NOTES: Day 1 (18-June-2009)

The Identity Services Summit in a Nutshell
* *Thomas J. Barton, Senior Director for Integration, University of Chicago*Q: how many projects are comfortable with our model for managing identity, per the "Enterprise IAM" slide in Tom's deck?

Project Assessments of Identity and Access Management Challenges: Kuali Projects
* *Ailish Byrne, Manager, ES Division, Indiana University* Jens Haeusser, Director, Strategy, The University of British Columbia Eric Westfall, Principal Systems Analyst/Programmer, Indiana University System*KIM (Kuali Identity Management) is a consumer of authentication, but does not provide this service. Thus it is authn-agnostic so as to enable plugging in to existing infrastructure.
Q: permissions v. responsibilities?
A: permissions allow action, responsibilities require action (e.g. in a workflow)
Q: Coeus and KIM?
A: They will be using it as part of their upcoming v2.0

Project Assessments of Identity and Access Management Challenges: Sakai and uPortal
* *Ray Davis, Programmer/Analyst, University of California, Berkeley_* Andrew Petro, Software Developer, Unicon, Inc._Note the MACE-paccman vocabulary effort underway, toward agreement on common terminology. See https://spaces.at.internet2.edu/x/qoI0

E.g. Kuali "responsibilities" maps to what?

Q: Could uPortal or Sakai consume an information model for roles and privileges?
A: Shared libraries would seem to be the direction to go for this...

Q: How quickly can you support a shared/harmonized vocabulary?
A: Kuali and uPortal would take some time, needing to incorporate it into the dev process, dependent upon significant input from stakeholders and consideration of key use cases.

Q: Next steps? Develop use cases using common vocabulary?
A: To the extent that the various projects are tackling similar issues, it would be helpful for them to coordinate and work together especially on the more complex cases.
Translating vocabulary between the various app/biz/functional communities and the developers is the challenge, esp. arriving at agreement on what are unique things...

Subjects/people/users would likely benefit from a common vocabulary as well.

Lightning Talks: Attendee Contributions to Identity and Access Management Challenges List
* *Grace Agnew, Rutgers University*

OLE Project
Most library content contracts differentiate access at on-site terminals v. remote access, in the latter case users must be authenticated.
Libraries tend to not have enduring patron files, as a privacy measure, with the exception of overdue books in which case the file remains open until resolved.

* *Jean-Marie Thia, National Tool for an Identity Repository* Jim Basney, TeraGrid and Open Science Grid*

Q: In the case of a PI sponsoring other project admins, who are likely to be e.g. grad students, what happens with their access when they leave the university? Or what happens when a PI leaves, or has dual affiliations?
A: Accounts have a one year lifespan, and PIs need to annually (re-) approve project members. Linked accounts are allowed, but a user can only link one, i.e. shared accounts are not permitted.

* *Gary Schwarz, RPI - Bedework*

Q: A common problem with *-DAV in general is that many require username/password authn. What are the major issues with Shib integration?
A: HTTP 302 redirection is sometimes not supported correctly. However there are *-DAV clients that do work with Shib, so the problems appear to be surmountable. There are HTTP clients other than browsers...

* *Stuart Sim, Kuali Student*Distilling the Themes and Developing Requirements

Breakout sessions

* *Session moderator: R.L. Morgan, Senior Technology Architect, University of Washington*

BREAKOUT: Integrating KIM with other identity services
Leader: Eric Westfall

1. Differences in Authorization Patterns
2. documentation on how to override KIM services for your own implementation
3. How implementable are KIM services, including terminology differences.

How can we enable the various projects to work together to solve these problems?
Integration of existing ID&AM services with KIM

Top Three Challenges:

1. Differences in Authorization Patterns
2. 2Adequate Documentation
3. How implementable are the KIM service

-
    - Differences in contracts
    - Differences in terminology

FOOTNOTE:
1. Scheduling time to work with other projects.

General Notes:
Challenges Integrating existing systems with KIM

Use Cases:
Ground Zero with kim, how complete is KIM as an IDM from the ground up.

- Answer: The services provided are complete for the Kuali use cases (which we feel the use cases are probably similar for other higher ed apps).
- KIM does not implement authentication services.
- KIM has roles managements
- Screens for managing attributes on Person
    - Name
    - Address
- Note: Most universities probably wont use all of the KIM reference implementations (although some may!)
- Kim's goal is to provide Service Contracts that handle various IDM concepts
- Kim will also provide out-of-the-box reference implementations the service
- Maintaining entity data is part of KIM

One solution for integrating for integrating with kim.

- Basically import data into KIM data structures
- 1. Port existing Role structure
- 2. Mange Role Structure
- 3. Creation of Accounts

Can KIM query existing systems to pull role information?

- Yes, it's currently implemented via the "Application Role". This allows for implementing institutions to pull external data.

What are the different KIM Services and what are some of their attributes.

- Identity Service: covers principals and entities
- Permission Service
    - Will make calls to the identity and role service
- Role Service -
- Group Service
    - Knows nothing about Roles

Q: What's the difference between roles and groups
Roles: Roles can contain Groups

Groups: applies no particular permissions.

How extensible is KIM at adapting to existing Rule System:

- Possible through the "Type Services"
- Allows you to pull external role information.

Can KIM talk to external SOAP services?

- Yes, through proper construction of the Type Service

Name spaces are used throughout KIM as a grouping mechanism.

- Are namespaces static?
    - Name spaces are maintainable and updateable.
- Uses of namespace
    - There is a permission that allows a person to submit to the workflow system
        - This would be namespaced to KEW

BREAKOUT: Issues in federation
Leader: RL "Bob" Morgan

1. provisioning and deprovisioning
2. harmonization across protocols, LoAs, and identifiers
3. Need for discovery services.

BREAKOUT: Collaborative Applications Framework (aka COmanage)
*Leader: Digant Kasundra*COmanage as a framework, an VM appliance with Sympa, Drupal, and Confluence, and as a service platform for collaboration communities

The appliance model would appeal to some organizations without this sort of established infrastructure.

As for calendaring, of interest would be publishing public events (e.g. via RSS or iCal). Bedework hasn't yet seen a federated use, even though some have successfully federated it. Subscription/access to public events does not require an authenticated account.

Federation low hanging fruit would be Calendar admins and personal calendars. Personal accounts allow customization profiles. RBAC would be desirable, rather than ACLs.

Standards compliance is important to Bedework...

iSchedule - server-to-server

In the COmanage framework, we are interested in looking at the range of ways that collaborative apps like Bedework can be deployed. A services interface that insulates the app from the framework would allow more flexibility.

For COmanage for a single collaboration, does it matter where the calendaring service would be housed - e.g. part of the appliance v. an externalized service?

Note different scenarios: federated access to a single COmanage instance v. COmanage as a managed collection of federated apps, located in various domains? In the latter case, discovery (e.g. personal calendars) becomes an issue, and is not in scope for the current work.

Note that the goal is to abstract out the authn/z from the various apps, that function having been delegated to the configurable "service" interface to the COmanage instance.

Top 3 issues:

1. Developing consensus around a common definition of a service layer. What other apps ought to be involved in this discussion, beyond the ones we are already working on (Sympa, Confluence, Drupal, Bedework)?
2. Scalability issues - including redundancy and availability
3. how to domesticate new apps (including devices? e.g. for scientific collaborations)

BREAKOUT: Roles and Permissions Ontology / MACE-paccman glossary

Leader: Leif Johansson

Top 3 issues:

1. what does the output look like?
2. Where should the work take place?
3. What's next?

dictionary analogy - definition and examples (use cases and requirements)

BREAKOUT: Kantara
Leader: Trent Adams

Top 3 issues:

1. what are the overlaps between I2 and Kantara working groups
2. What resources can Kantara bring to bear?
3. What would be the utility of the output?

BREAKOUT: Groups, Roles, and KIM/Sakai
Leader: Tom Barton

Top 3 issues:

1. recognition that there is commonality about groups in various app contexts - thus ought to be a fluid component for group selection
2. terminology issues
3. proper roles of group and role management practices

BREAKOUT: Microsoft
DotNet Point of view:
Microsoft is starting to embrace the .NET. Why don't we use Geneva? For DOTNET, then asapi for old stuff.

Top 3 issues:

1. Authentication Focus
2. Attribute Issues for rules.
    a. Supported by Shib Dotnet
    b. Attribute Group Mapping
        i. Role Provider "Shib" attributes to "Role"
        ii. In XML / Config File
3. Do we tell people to buy into Microsoft's frameworks, and along that line just buy into Geneva. Build a community around what we do have.

Goal to get a header collection like return from the client. Security of IIS headers. Do we just want to use Geneva.
Projects will invest time in stuff that succeeds in the community.
Drop in replacement for different federation/SSO technologies.

BREAKOUT: Calendaring
Top 3 issues:

1. federated authn both for a browser and non-browser environment
2. role of roles in calendaring for access control
3. standard service for discovery of profile info about individuals, irrespective of whether it is stored in a social network or a campus directory. XRS and XRDI were discussed as example solutions...

NOTES: Day 2 (19-June-2009)

Lightning Talks
Q: CAS and Shibboleth seem to be nearing each other in functionality, should they merge?

A (Shib): There is currently no projected overlap on the SP side. If MyCAS were to support SAML that would be a significant step, but that doesn't appear to be on the roadmap.
The XRD community looking at accepting constrained SAML signatures is interesting, pending code. At that point it should be relatively easy to enable SAML support in CAS.
On the IdP (Java) side, there is some code-sharing happening now in terms of reusing libraries, and perhaps CAS could leverage the Shib attribute infrastructure.
On the SP side, the projects offer different models as CAS needs to be integrated with the apps, while Shib is isolated outside.
It is likely that SAML support in CAS will be operationally consistent with Shib, due to the communication between the projects.

A (CAS): We are expanding protocol support to give more options (esp. on the client side), and would leverage existing OpenSAML work. There doesn't seem to be logic in merging the projects at this point, given the need to support the installed base in forthcoming releases.

Q: Re: Grouper and Kuali integration, where how to best track this and get engaged?
A: The Kuali and Grouper wikis both contain relevant info, and both project mailing lists would be logical places to house this. It would make sense to create a dedicated area for this in one of those wikis.

Q: COmanage and KIM, what is the potential for integration?
A: Too early to say, but it looks promising. KIM seems more focused on ERP-type systems at the moment, while COmanage is focused on collaboration, but there may be opportunities ongoing.
Sakai might also be a candidate for integration with KIM. Service modeling and interface development has been happening separately in the projects, but in many ways tackling similar problems and service contracts.
Improving collaboration between all of the identity-based projects (both producers and consumers) would benefit all...
Working code and deployed systems are essential to make progress...

Q: Roles and permissions in Spring?
A: Spring security mostly deals with authn/z, but really just for Spring-based apps. There are integration points for CAS and SiteMinder, among others, and there is thought being given to abstracting roles and permissions to one level. The Shib IdP and Kuali are Spring-based.

Q: What about Spring security roles mapping to Grouper or perMIT?
A: This seems like a good idea for Grouper, but perhaps the bigger question is what should be the groups service framework appropriate for various apps? uPortal uses Spring, but doesn't yet use Spring security.

MIT has a number of Spring security apps, both internally developed and not. The issue would be getting code that everyone would be happy with to incorporate into various distributions.
Note that Spring security is just a library, and there would likely be other things to look at such as servlet containers.

FINAL SESSION - CONCLUSIONS, NEXT STEPS/FOLLOWUP

MACE-paccman seems to be the right setting in which to pursue topics around groups and roles, at least initially. The glossary and ontology of access management terms and concepts are key...

Business benefits from the Kantara perspective - this is a way of reducing friction when developing or buying or integrating a new system.
*Followup by: Leif Johansson, Trent Adams, Michael Pelikan, Paul Hill, Tom Dopirak, Ray Davis*Q: is there a way of soliciting participation from other large projects in higher-ed? E.g. Kuali?
A: Kuali is participating in MACE-paccman already. They will look at pulling other team members into that. Rice and KIM seem to be likely candidates, in particular.

Translation among Sakai, perMIT, paccman, Kuali terms
Followup by: Ray Davis, Eric Westfall, Jens Haeusser, Scott Battaglia + other Kuali TBD, Spring security folks

Grouper/KIM service integration
*Followup by: Tom Barton, Eric Westfall*Service interfaces across projects would be a good area to focus on, and MACE-paccman seems to be the logical forum for this.

Q: Does MACE-paccman have subgroups focused on various topics?

A: Not yet, we would want to see significant energy around a particular topic before spinning up subgroups, v. focusing particular calls on a topic for the whole group.

Re: service contracts: collate, examine for commonalities, make recommendations, refine...
Followup by: Benn Oshrin, RL "Bob", Jens Haeusser, Tom Barton, Digant Kasundra

CASified, Shib-enabled .Net, or SharePoint
CAS community effort
Followup by: Jean-Marie Thia, BillT, Scott Cantor

Federation considerations, SAML-specific and otherwise
Document what it means to federate...
*Followup by: RL "Bob", Trent?, Eric Westfall (Kuali Research Admin system case study?), Scott Cantor, Renee Shuey, Digant Kasundra*It would be good to hold this discussion in the wider venue, to include as many communities and projects as possible. E.g. Concordia

COmanage
Bedework <-> COmanage discovery, clarify a services layer and rold structure for Bedework
Federated AuthZ in the non-browser case
Build relationships between CalConnect, IETF, federated IdM communities
Followup by: Gary Schwartz, Trent, Leif Johansson, Ken Klingenstein

How do we continue and organize the community represented at ACamp?
Enhance dev framework with roles etc.
Spring, GoogleApps, Python, Ruby ? - django, twisted, rails, PHP already done?
Followup by: AndrewP, Scott Battaglia (Spring Security), Leif and Roland ? (django), Steven Carmody, RL "Bob", and RayD / Sakai folks (Google)

How do we stay informed and involved in all of this, and coordinate among the projects?
IdM central clearinghouse - collate work of this community.
Potentially host under Jasig, Kantara, or MACE/Internet2
Followup by: Jens, Tom Dopirak, Trent ? , RL "Bob"

Future events for followup, including:

- Jasig unconference Sep 28-30, 2009, U. Illinois, and annual conference March 2010 San Diego
- Also on these dates is the GSA-sponsored "Tao of Attributes" workshop
- Kuali Nov 17-18, San Antonio
- I2 Member Meeting, October 5-8, 2009, San Antonio

General Observations...

- CIOs are tending to be less strategic, in general, and this trend places more focus on those who are remaining... They will be very demanding of our community, to work together on these issues.
- An anticipated common concern is how fragile this work is, how shallow the pool of key players is. There is not much of a farm system in place
- A gap analysis hasn't really been done, looking for key infrastructure pieces missing. An example is diagnostics, or even a common format for log files...
- Also note key players not yet at the table, e.g. the science communities including physics and plant biology, that CIOs need to support.
- This is becoming a more international community, and we will likely depend more upon them for contributions ongoing.
- The upcoming "Tao of Attributes" workshop will be an important window into a key area... It will be netcast, details forthcoming.