Conference Call Minutes, 14-July-2008

SharePoint Working Group Minutes, July 14, 2008

Attending

Mike Grady, University of Illinois at Urbana-Champaign (chair)
Debbie Bucci, National Institutes of Health
Scott Cantor, Ohio State University
Rick Downs, University of Virginia
Khoa Le, National Institutes of Health
Tim Newcomb, Committee on Institutional Cooperation (CIC)
Greg Nims, Committee on Institutional Cooperation (CIC)
Chris Pruess, University of Iowa
Gary Rogers, University of Iowa
Galen Rafferty, Committee on Institutional Cooperation (CIC)
Nick Roy, University of Iowa
Steve Olshansky, Internet2
Ann West, EDUCAUSE/Internet2
Vincent Wong, National Institutes of Health
Dean Woodbeck, Internet2

NIH Deployment

Licensing

Part of the SharePoint team from the National Institutes of Health joined the call to discuss the status of their first federated SharePoint instance. The PIONet service, consisting of public information officers, will be the first application to be federated. NIH is using the SiteMinder SSO, which can be accessed by institutions running Shibboleth.

There was a discussion about the necessary Microsoft licenses. It is NIH's intent that the application owner, in this case the NIH department developing PIONet, will be responsible for purchasing the appropriate SharePoint licenses. Microsoft offers a license that will accommodate all external users of the application.

Should, at some point, a university decide to set up a SharePoint application within NIH, that university would own the application and be responsible for the license.

Identifying PIOs

There was extensive discussion about how, in this instance, NIH would identity PIOs for the application and, in a broader sense, how people would be authorized to use federated NIH SharePoint applications

Using PIONet as an example, there can be multiple people from one IdP having access. At this point, NIH has a list of participating institutions and will be working to identify the proper people. There are concerns about the security and scalability of the system. At this point, NIH has not negotiated any attributes that would assert someone as a PIO.

NIH uses Active Directory Application Module (ADAM), which draws information from the SSO (SiteMinder) team, including email, FirstName and LastName; and could send any security roles or work with LoA. Access levels could be based on LoAs. ADAM allows assignments to groups, which manages access. Using different levels of assurance is not anticipated for the PIO application, but there may be a use-case in the future that requires a higher LoA.

At this point, provisioning is a manual process at NIH, using SQL and replicating that information to ADAM. An individual at NIH then puts the user into the SharePoint environment. It is NIH's intent to have a gatekeeper for each application. Gatekeepers would help manage the application site and give permissions to users wanting access.

In addition, SharePoint itself has multiple levels of authorization. A user can be simply a reader, with the ability to see documents, but not change them; all the way up to someone with full control. At this point, the gatekeepers must define that role for each individual. One approach may be to provision all of an institution's faculty as "readers," but a gatekeeper would need to provide higher levels of access and control.

There was a general consensus that, while most institutions aren't maintaining an attribute that would identify a PIO, provisioning via attributes seems the best way to handle this, allowing it to scale. For applications attracting large numbers of users, the community could agree on a profile on who an institution would assert, for example, as a faculty member.

There are some needs emerging in this use-case that will need to be addressed other than by Shibboleth. Grouper may prove useful, for example, as a way for IdPs to manage entitlements, rather than doing it on the NIH side. Membership in a group in the IdM could be used to assert an attribute. For Shibboleth, it will be necessary to assume that IdPs will assert based on eduPerson schema, otherwise there is not a good way to do automated authentication.

User Support

Another issue discussed was educating users about where to go for support. If a university's IdM goes down, for example, NIH doesn't want users inundating them. The community recognizes this as an issue, but there are not any best practices formed at this point. One such practice might be that, to use a mission critical application, an IdP would need to assert that its IdM system will be up and working a certain percentage of time. With an increasing use of federated authentication at institutions, this will become more of an issue.

Debbie Bucci said that NIH has started compiling a list of trouble-shooting steps as they provide user support. She will share what they have with the list or on the wiki.

Building the SharePoint Wiki

One of the goals for the working group is to develop a wealth of information on the wiki.:

- Build a set of use-cases
- Gather examples of practices and policies around the use of SharePoint
- List how universities are using, or how they plan to use, SharePoint, both internally and federated. What SharePoint tools are you using now?
- Recipes for provisioning around authentication and the use of attributes

Mike Grady encourages all working group members to provide any information that fits these categories, or to introduce new categories on ways to encourage collaboration using SharePoint, on the wiki.
https://spaces.at.internet2.edu/display/InCCollaborate/InC-SharePoint

Debbie Bucci said she would help by demonstrating how SharePoint is being used across NIH. Vincent Wong has taught a lot of SharePoint courses at NIH and how they use it for collaboration over the Internet and how it ties in with the Microsoft Office suite.

Mike Grady said he knows of instances on how SharePoint is being used at the University of Illinois and at the CIC.

Next Call

Mike Grady indicated the next call may include a demonstration of work done at the University of Illinois using ADFS, as well as continued discussion on attributes and authorization.

The next call is scheduled for July 28, at 2 p.m. EDT.