

CAMP Shibboleth: Flexible Web Based Authentication and Authorization  
Hilton Portland and Executive Tower, Portland, Oregon  
Tuesday, June 26, 2007

### **Management Discussion for Deployed Campuses: Web SSO**

10:15 a.m. - 11:30 a.m., Management Track

Speaker: Michael R. Gettes, Manager, Applied Middleware, Internet2

Scribe: Jessica Bibbee, Technical Analyst, Internet2

#### Abstract

Following up on the previous topic, this discussion session will explore the issues and strategies presented. In particular, the group will consider institutional practices and determine if commonalities exist.

#### Discussion

{Albert Wu} of UCLA expressed concerns over privacy in the wake of recent data spills. He was curious about how others addressed minimum security standards from the policy side. UCLA is not a centrally managed campus; Internal Audit has focused on major business applications, but has yet to address the main campus. It is a challenge to get Audit to consider Identity Management as a major business area.

Good relationships are key; others must have a solid understanding of the technical issues. Where Audit hires more IT savvy staff, there is faster uptake of these issues and concerns.

What is the best way to deal with the challenges around non-web-based applications? What are the larger strategies of identity management? How to meet the needs of the multi-faceted areas of campus?

There are several options for signon, including Shibboleth, another SSO, central LDAP AuthN, etc. Attendees reported that while some policies are posted on the web, others are by word of mouth. IT is accountable for speaking to those who violate policies. By extending the use of LDAP to other departments, you need to consider the trade off of user experience vs. security.

{Michael} asked if anyone had considered or tried Xythos < <http://www.xythos.com> > for file sharing. UCLA has at some point, though {Albert} could not report on the current usage. He did say that they have 20-30 different class website systems with varying implementations and technologies, which they are now trying to consolidate. While they are clear on what they want with respect to central identity, it does not translate as easily to the applications hosting. It is not advisable to have a site request username/password, though exceptions must be made. Some medical centers and business schools are trying to establish separate identity.

{Mitchelle Morrison} of MUSC said they have provisioned Kerberos as a back up, but are not using it now. They are in the process of rolling out Shibboleth, focusing on a new governance structure. Only recently has there been consensus with an understanding around the Identity Management structure.

{Albert} pointed out the difficulty around merging logon IDs as account provisioning standards vary widely. Some require security training before acquiring a logon ID, but they cannot require this of all. {Klara} suggested dove-tailing this process with a centralized card-system. {Zephyr McLaughlin} of U. Washington mentioned the lower level of assurance associated with, e.g., library access, and the need to communicate that to applications. Registration is only the first piece; what happens if someone loses a card – is it simply a bookkeeping issue? Flexibility must be designed into the process to accommodate various systems until they align.

Another issue is how to securely administer accounts and manage the root policies without compromising all systems should root itself be compromised. If we do not synchronize passwords for people, they will do it themselves, creating unnecessary exposure.

How to effectively start doing SSO in a feasible manner? Begin by educating the various people in technologies, knowing that vendors may not be supportive. Even more important is the need to establish good practices, i.e., forming a closer relationship with the help desk doing Identity Management.

Attendees expressed greatest concern around the management of Shibboleth deployment in getting the data stewards to care about the ARPs. Their time is limited, and subsequently SSO becomes a burden in addition to their core responsibilities.

{Michael} asked about existing policy and practice: Are attributes given to anyone who asks, and is the transaction documented, including to whom? The responses were mixed – sometimes the transaction is documented, but not always the reasons why.

#### Additional Resources

Kevin Marooney's LibertyRoad blog at PSU - <http://www.personal.psu.edu/kxm/blogs/LibertyRoad/>