Shibboleth CAMP Session June 29th, 2004
Management Track: Targets: The Requirements of Participating in Federations
Nathan Dors, University of Washington
David Yakimischak, JSTOR

Nathan Dors talked about the role of Central IT in delegated management structures and how to successfully deploy targets. One distinction is to understand the difference between multi-institutional and multi-campus.

Q: Is there anticipation that many campus targets will join InCommon? Why would they need to be federated outside the university?

They may have their own identity, for example the Center for the American West at the University of Colorado has an identity distinct and separate from the university.

Pricing and a mechanism for registering resource providers will be needed. The goal of pricing is cost recovery not revenue. For campus resource providers there is the issue of attribute leakage. Are you comfortable speaking for a procedural unit of your campus under your origin registration? If the relationship is only tangential then they should be registered as a separate target, not under the campus origin registration.

Q: Where is policy set? How is misuse of a system identified and the abusing user shut down?

If JSTOR detects an IP address with massive downloading they contact the business person at the university so action can be taken by the university. The university and JSTOR work together to address the issue.

Q: How is handled when there is no contract/ out of band agreement on process?

Currently how such dispute resolution would be handled hasn’t been addressed, but it would be between the two entities involved, and not the federation and the entities.

The focus is on how to minimize risk but it should not be confused with a secure solution, which is not what is being offered.

There is concern people may lose track of the provenance of a digital object. There is a need to be careful to protect the provenance of an object. Shib only protects a small part of a larger policy space of contracts. There will be log files in InCommon but access is a concern since the details contained in the logs will compromise privacy. Shib can be used to access the log files to avoid compromising policies in place.

David Yakimischak, JSTOR

Currently 90% plus of JSTOR’s authentication is by IP addresses. Logs are checked hourly for possible access abuse. Physical location does not always define access privileges. JSTOR would like to move away from IP based authentication.

Q: What is an entitlement?

An entitlement is a trusted outsourcing backed up by a contract. It is a riskier way of describing who has access to the resource. Entitlements are a good thing but require a higher level of trust. If you don’t trust the attribute why trust the entitlement? Because the entitlement is a local way to pass authorization.

The motivation to change to a new mode of authentication is that it must be better, cheaper or both.
Q: Is there a lot of variation in how attributes, such as faculty, staff, and student are being populated?

There is some variation. The desire is for a persistent opaque identifier to show how the service is being used and to identify abusers.

Q: When an instruction is detected can you block a user?

In the current IP world you can’t really stop them. Shib provides a major authenticated step forward. Currently you can inform the institution and work with them to take steps to stop abuse. If the institution does not take any action then there is the option of legal recourse. Shib also enables other attributes such as ADA enhancements, and localized language.

Q: Do we need members to post their policies about persistent id's?

It is dependent on what is in eduPerson and over what period of time the id persists.