Minutes from Vendor subgroup call 9-11-09

Notes: Conference call 9-11-09

Vendor subgroup minutes

Attendees:

Dean Woodbeck, Internet2
Foster Zhang, JHU
John Kiser, UPenn
Andy Ingham, UNC
Jonathan Lavigne, Stanford
Ann West, Internet2
Fred Zhang, Michigan State
David Kennedy, Duke
Ron Snyder, JSTOR
Spencer Thomas, JSTOR

notes - kennedy

AGENDA

Pre-reading:
https://spaces.at.internet2.edu/display/inclibrary/Best+Practices
https://spaces.at.internet2.edu/display/inclibrary/RegistryOfResources

Introductions
- including brief overview of InCommon Library Services Collaboration

JSTOR
- overview of Shibboleth implementation
- usage of Shibboleth SP software (SessionInitiators?)
- implementation of WAYFless URLs and direct links to resources
- what has or hasn't worked

Topics for discussion:

Best Practices
- are these feasible for resource providers
- do these make sense
- thoughts on how to go about making this best practice amongst resource providers

What role should InCommon or the InCommon Library Services Collaboration play?
- policy setters
- documenters
- testers
- implementation documentation/assistance

Is there a desire/need for standardization across federation members' identity provider implementations that would simplify the process for resource providers' configurations?

What are we missing, especially things that you have learned from dealing with other federations besides InCommon?

NOTES FROM DISCUSSION

Kennedy gave an overview of InCommon Library Services Collaboration and vendor subgroup activities

JSTOR history and implementation
Thomas recounted JSTOR's involvement with Shibboleth. JSTOR has been involved since the conceptual stages of Shibboleth. Recognized at an early stage some of the looming problems with IP validation. Popular use of EZproxy amongst customers, but did not change much the IP validation picture. Rolled out Shibboleth SP 1.3, and later wrote a customized SAML implementation with Shibboleth extension that could work within a Java servlet environment.

JSTOR participated in the creation of the common-lib-terms and the standardization around eduPersonEntitlement usage.

JSTOR recognized early on the need to support deep links or authenticated links directly to individual journals and has supported that from the beginning. By the same token, they recognized early on that they needed to support WAYFless links and have done so from their initial Shibboleth implementation.

JSTOR supports 5 different forms of authentication, of which Shibboleth is one.

In terms of what has or hasn't worked, the things that haven't worked have been fairly technical issues, due mostly to the nature of having a non-standard implementation.

Experience related to multiple federations
There has been a significant uptake on Shibboleth in the UK. This due in large part to JISC no longer funding access to Athens and providing funds to move institutions to Shibboleth

There has been a slower uptake here in the US.

German federation was more strictly Shib 2.0, and that caused some complications for them, but nothing major.

Among federations, a lot like InCommon. Learned with the UK, that having encouragement/incentive to switch to Shibboleth made all of the difference in their case.

Best Practices
Agreement that it is appropriate for the federation to set expectations and best practices for the interations between member's implementations. JSTOR indicated general support for our group creating best practices as well as the best practices that have been identified.

In terms of how these best practices compare with other federations, Thomas didn't know of complimentary best practices at least not in the UK.

Regarding the document itself, it is good to give examples, but risk losing the audience if it becomes lengthy.

Best Practices - attributes
Discussion around the use of eduPersonEntitlement. JSTOR very much in favor of this attribute over other options, such as eduPersonScopedAffiliation. It actually simplifies the interaction on both ends, identity provider and service provider, with the recognition that there is probably more startup to implement the eduPersonEntitlement attribute on the IdP side.

Regarding personalization, JSTOR is not currently using personalization features of Shibboleth directly. They have future plans to integrate Shibboleth personalization attributes with their current JSTOR user accounts, but haven't analyzed yet whether or not they will use targetedID or principal name. Is there a reason for one over the other. Thomas pointed out that it comes down to an issue of privacy vs functionality. Depends if you want to relate user accounts from one service provider to user accounts of another service provider. They will likely be dealing with this issue when interoperating with related platforms.

Best practices - wayfless
JSTOR has been doing this from the get go and support it being included in best practices. It is hard to say if the language is sensible to someone without a lot of experience in this arena, because JSTOR is already familiar with a lot of the terminology.

Best practices - Shibboleth/EZproxy hybrid
This was something JSTOR hadn't seen before, but Thomas indicated that this provides a good transition for institutions.

Discussed the larger issue of navigation if user navigates, unauthenticated to JSTOR or any service provider, and the service provider has to lead the user to their authentication mechanism.

Commonality/standardization across identity provider implementations
Beyond eduPersonEntitlement, JSTOR asks for very little in terms of user attributes. For this reason, they have not seen a need for more standardization. There might be a different response from other service providers that are more attribute-intensive

Identity provider focus
From the Service Provider perspective, Thomas mentioned the value he sees in giving people recipes, or some amount of hand holding for getting things set up on the identity provider side. And he recognized some of the CAMPs and efforts InCommon has put into this. Our group sees the registry as part of the information that would be useful to identity providers in this regard.

There has been a tendency among this group to focus on the service provider end. But there has to be buy in at the university level, or there is no start up.

Additional takeaways

From the service provider end, there is a recognition that nobody is going to be 100%. This is in terms of enforcing contracts, whether via IP validation or through granting entitlement values or assigning affiliate attributes. A lot of this comes down to trust. Trust that has been established already with agreements over how institutions are enforcing authentication via proxies and IP ranges. The arrangements or details change with Shibboleth, but it is the same idea of vendor trusting the university.