TechIssues

Technical Issues Submitted by Campuses

We need to be able to continue our current level of functionality under a load-balancing environment.

Many sites are currently running a Shibboleth IdP in a load balanced environment. Information is available here.

We need to figure out how to use one (1) IdP for multiple trust relationships, or to manage IdP instances for different trust relationships. One of the issues is that not all trust partners seem to trust the same Certificate Authorities. That means different SPs may need to see different certs, which in turn means having different instances of the IdP so we can present different certs. Unless some trust partners change their policies. E.g. InCommon seems to only recognize the InCommon CA, but InCommon is not our only trust relationship, and we cannot expect the other trust partners to accept the InCommon CA.

To use different credentials with different Relying Parties, use multiple RelyingParty elements in your idp.xml file Info available here.

For some SPs, we want different access for walk-up patrons vs. remote patrons. That is, while patrons who are not physically present must present authentication credentials, we want patrons in the library or on campus to be authorized because of their physical location.

A writeup describing the approach implemented by the Univ. of Wash. is available here.

At least one service we want to use Shibboleth with do not yet formally support it, but has informal support and can not yet receive attributes.

Not sure what "informal support" means...

There are some special cases where authorization relies on information not contained in the campus IdP. For example, alumni who have paid for borrowing privileges are eligible to use Interlibrary Loan, but the campus IdP does not have this information (nor should it); students working as research assistants often act as proxies for faculty, and so have two roles which must be kept distinct. (We plan to work with the campus IdP for most cases, and deal with special cases through some other mechanism.)

Is this an issue for the group?

Libraries as Service Providers (UCSD – a library has a web service that they would like to secure and manage access to with Shib. One case we have now is a MediaWiki instance that we would like to keep confined to just UCSD Libraries staff. Another example is switching from barcodes to SSO for item checkout through our OPAC.)

Specific Issues here? staff tech training? others?

How will places like the library set up affiliates on the fly? (UCSD working on a web service)

Depends on local campus IdM software.

Shib doesn't really have a standard logout method

Sorry for the zen – what would logout "do"?

(UMD) We use a gateway software, Metalib, that is Shibbolized. Metalib is used as the access point to online resources, and provides users with URLs to get to the online resources. However, Metalib does not prefix these URLs with the appropriate Shib IdP prefix in order to properly SSO authenticate the user at the online resource SP.

Sounds like we want Metalib to do what EZProxy will be doing....