Technology Approaches Organized by Areas of Interest

Background

A question that we need to ask ourselves is why do we need to document various technology approaches and their associated use cases? The answer is simple, we need to create an understanding of the benefits of using Shibboleth to solve issues of managing resource access. Several other specific reasons that we have identified are: use cases are meant to help make a policy decision to shibboleth enable a resource, use cases also assist in trying to promote this technology to the administration, third it helps people formulate internal policy, and finally use cases are less focused on a specific technology and more focus on the user of the library and how they utilize the library to meet their needs.

We also wish to generate documentation to support cookbook solutions to many of the use cases below. Also as a result of clarifying use cases we hope to attract additional shibboleth enabled (and to-be-shibboleth-enabled) vendors to InCommon and thereby to the member institutions of InCommon. We need to identify additional local applications directly supported by libraries and/or other large intra-university divisions who support various library functions.

A large portion of the use cases touch on various aspects that will require Shibboleth enabling the proxy system. We need to investigate the "friends of the library" & POI groups (as well as others as of yet unidentified groups) into the Shibbolized access to resources (for libraries currently, these groups are only stored in the library ILS system). Eventually we need to reconcile campus federations and the InCommon federation.

Another big issue to investigate are Federated Service Providers. At present there are approximately 100 information providers in the U.K. federation; the U.S. lags in getting vendors into InCommon. At Brown, for example, the librarians believe that getting the 15-20 most-used external resources Shib-enabled would take 90-95 percent of the traffic off the proxy server. On customer surveys, users complain more about the proxy than everything else combined.

Also, regarding ARPs and Privacy Tags, due to the laborious requirements of releasing information fields that are stored in LDAP it would behoove us to look at ways to determine how to handle having users make decisions about which attributes third-party providers will receive. Brown is most of the way through a deployment of uApprove, which allows users to see which attributes are about to be released and to approve/disapprove. These processes will require education of the users as to the process, but also that disapproval will prevent access.

The first product of the following uses cases should be a "Getting Started Guide" which helps to outline what steps a user should take to resolve the issues explored here. Keep in mind that though a lot of these use cases relate specifically to libraries, it is possible to extrapolate to other portions of a university or institution that have similar needs.

Bedtime Story

What is a Bedtime Story?

A "bedtime story" states, in simple and clear language, what experience performing a certain set of actions a user wants. It is a starting point that describes a mostly idealized series of events which subsequently assist in identifying how one or more current technologies support a process; as well as potentially identifying some failures or absences in currently available technologies.

UML Diagram

What is a UML Diagram?

Garnered from wikipedia: http://en.wikipedia.org/wiki/Unified_Modeling_Language

The pertinant piece to understand is that, UML offers a standard way to visualize a system's architectural blueprint, including multiple elements. The term stands for Unified Modeling Language, and we are using a small piece of the overall system to help diagram the architecture that supports the processes first described in a bedtime story and then broken down into component parts in the use cases.

Shibboleth-EZProxy Hybrid Use Cases

Jane is sitting at Starbucks following her Bio 301 class; she's reviewing the work she'll need to do before the next class meeting.

She goes to the campus LMS system, logs in with her University web single sign-on userid and password, and starts viewing the course information.

There are three articles she has to read -- she clicks the link for each one, and is taken directly to articles at Elsevier, EBSCO, and JSTOR. She doesn't have to identify herself because all three sites operate within the same Web SSO framework that is used on the campus. All three links are "deep links" -- they take her directly to an article deep in the site, rather than to the site's front page (where she'd then have to search for the desired article).

She decides that she'll also search for additional articles on the same topic. She goes to MedLine (an abstracts DB), and starts searching. She finds an interesting article, and clicks the OpenURL button. She is redirected to the Link Resolver at her campus, and on to the deep link at "Biochemistry and cell biology"; once again, she doesn't have to identify herself.

She also decides to search the local campus library catalog for relevant books. She finds one -- but when she logs in to the local ILS system she discovers that one of her classmates has already checked the book out. She clicks a button, tho, and is taken to Iliad (the inter-library loan system). Once again, she doesn't have to identify herself. She orders the book from another campus library.

Lastly, she goes to XXXX site. Once again, she doesn't have to identify herself. This site is able to use the persistent but anonymous identifier sent by her campus to uniquely identify her. The site doesn't know her real identity, but recognizes that "its her" whenever she returns. She's able to save searches from one session to the next, and create a personalized look to the site. If she were willing to share her email address, the site would send her a monthly email newsletter (with content tailored to her searches).

Note: the following two use cases are adaptations of the "bedtime story," broken down into distinct use cases. Please remove this note once the use cases have been accepted.

1. **Student Access to Library Searches with SSO** Jane is in the library ready to do research for her Bio 301 class. She has three articles to read that are all available online. Fortunately, the library at Mass State U subscribes to all of the databases she will need. While she doesn't realize it (nor does she need to), each article comes from a different database provider: Elsevier, EBSCO, and JSTOR. The ideal situation is for Jane to be able to reach all three articles directly, without having to sign on to three different services and without having to do a search once she gets to a database (in other words, she access the article's "deep link" directly). She also thinks it would be nice to be able to save her search for future visits.
    a. UML Flow Diagrams for EZProxy
    b. N.C. State Case Study
    c. University of Chicago Case Study
    d. University of Maryland Case Study
    e. MIT Case Study
2. Jane now decides that, while she is in search mode, she will look for additional articles for her topic. She goes to MedLine (an abstracts DB), and starts searching. She finds an interesting article, and clicks the OpenURL button. She is able to access the article, again directly and without having to sign in again.
3. Still motivated to search, Jane goes to the campus library catalog to look for relevant books. The books she needs are either checked out or are not available locally. She clicks a button and is taken to the inter-library loan system. She is able to order the books via the loan system without having to sign in again.
4. **Faculty member is unable to leave their office** Professor Moriarity has a deadline to meet and doesn't have time to get to the campus library. He signs on to the library's catalog from his office computer and does a search for the book and article he needs to complete his NSF proposal. He finds the book in the library catalog and checks a box to take advantage of the library's campus delivery service. The prof finds the article in one of the databases to which the library subscribes. He accesses that database without needing to sign in again. He is taken directly to the article, without having to go to the database provider's home page.
5. **Anonymous Personalization** (Many vendors support a personalized experience for users; allowing them to set preferences and save searches. This personalized experiences requires the users to create a userid and password with the vendor.) Jane Doe and is taken to Service X (she was routed through the campus IdP, but had previously authenticated). The IdP releases persistentID (opaque identifier) and eppn (primary user identifier - not anonymous) to Service X. First time access with these identifiers creates the Service X account; subsequent accesses the same Service X account.
6. Traveling between sites in a Hybrid environment? (Either number 2 or a new writeup)

ILS Use Cases

Jessi has just come to the library after receiving a list of books that she needs for the semester.

She is sitting in front of one of the Library computers that students use to search the library resources. Looking at her list of books she notices that they fall into two distinct groups. Some of the books are only for withdrawal from Library Reserves while other books will be needed for the entire duration of the class.

Without logging into the ILS she searches for the books that she needs. She's gotten lucky and four of the six books that she needs for the semester are owned by the library. However, one is still on loan and due to be returned in three days. She clicks to add it to her e-shelf (or e-cart) to place it on hold, at this point she is prompted to login and does so. After going back to her search and adding the other three books to her e-shelf for printout so that she can go track them down, she decides its time to check inter-library loan in the hopes that she can find the last two books which her library doesn't own.

Her luck holds and she finds that several potential members of her library's peer community have the books for withdrawal. She now switches to using the ILLiad system without having to log in. She places a request for the books and waits until hearing back from them later in the day that the request has been accepted and the books shall ship in the next few days.

Finally, she logs into her schools Course Reserves system that houses a complete list of all the materials and books that she will need for her classes. Again, there is no need to login as her initial login is still useful. She puts in a request for the materials she needs, logs off and heads up to the Reserves department to pick the materials up at the scheduled time.

1. **Authenticate campus community members and friends of the library (only in the ILS system)** some text

User Walk In Use Cases

1. **Library Walk-in user**
    a. User authenticates using their campus-issued credentials
        i. **(authN via Web SSO) Campus Community Member using public machine in the library** User logs in to the machine using their campus issued credentials and a standard desktop login process; this gives them access to their network-based file space, etc, and perhaps other permissions on the desktop machine. They access licensed material, are redirected to the campus IdP, authenticate once, and are redirected back to the resource. Subsequent access to other licensed material does not require additional authentication events.
        ii. **(authN via Desktop login) Campus Community Member using public machine in the library** User logs in to the machine using their campus issued credentials and a standard desktop login process; this gives them access to their network-based file space, etc, and perhaps other permissions on the desktop machine. This also stores a Kerberos ticket in the desktop. They access licensed material, are redirected to the campus IdP, are auto-magically authenticated using SPEGNO/K ticket, and are redirected back to the resource. Subsequent access to other licensed material does not require additional authentication events.
    b. User authenticated using credentials other than their campus-issued credentials
        i. **(Login via IP address)** a walkin user sits at an "open access" machine in the library. No login is required to use the machine. The user attempts to access licensed material, are redirected to the campus IdP, are auto-magically authenticated using the

Univ of Washington's mod_auth_location apache plugin (http://staff.washington.edu/fox/authlocation/); it maps an IP address to a user identity (eg GUEST1, which possesses a specific set of permissions, perhaps less than a community member), and are redirected back to the resource.

ii. **(Librarian does login for user)** a walkin user sits at an "open access" machine in the library. A library staff member logs them into the machine. The user attempts to access licensed material, are redirected to the campus IdP, are auto-magically authenticated to the Shibboleth IdP using SPNEGO and the desktop credentials,which possesses a specific set of permissions, perhaps less than a community member, and are redirected back to the resource.

Multi-campus and Consortium Use Cases

Note: These use cases assume that the necessary entitlements have been provisioned to the users.

1. **Multi-campus/consortium and multiple IdPs**
   a. **Separate Licenses**
   Jane is a staff member at a University Medical Center. She is also taking classes at the local campus of that same University. Jane has been issued two digital identities - one for the Medical Center and one for the University. Her Medical Center identity provides access to resources licensed to the Medical Center and her University digital identity gives her access to resources available to the University community. Note: Some of the resource licensed to the University are not available to Medical Center. Jane oftentimes finds herself switching back and forth between her digital identities depending on her research needs. Jane wishes she could link her digital identities together and then the appropriate entitlements would be available to access resources. The entitlements would be a mashup of her entitlements for the two identities.
   b. **Multiple licenses with one vendor**
   Steve is a staff member at a University. He is also a member of a local consortium. Steve has been issued two digital identities - one for the University and one for the consortium. His University identity provides access to resources licensed to the University and his consortium digital identity gives him access to resources available to the consortium. Both groups provide access to resources at vendor Q but the consortium offers more content at vendor Q. Steve oftentimes finds himself switching back and forth between his digital identities depending on his needs. Steve wishes he could link his digital identities together and then the appropriate entitlements would be available to access the resources. The entitlements would be a mashup of his entitlements for the two identities.
   c. **Virtual Organizations**
   Sam (faculty member at University A), Joe (staff member at University B) and Pete (a Program Director at NSF) are collaborating on a research grant. As members of the research team they are entitled to access research articles that are not available at their associated institutions. Each member of the research team prefers to use their institutional digital credentials when accessing research material and they have a need to access research material anywhere.
   d. **Collaborative projects within Federations**
   Chris (faculty member at University A) and Mark (staff member at University B) are collaborating with other individuals of a Federation like InCommon on a variety of issues. They need a space where they can post meeting minutes, software, reports and evaluations. They want to use their respective organization's digital credentials to access the space. This wiki space is an example of this use case.
   e. **University Organization as SP**
   Char (staff member at University A), Sue (staff member in Organization B) and Jen (a University C) have access to a SP running at University C. The University A and C are in a Federation similar to the CIC and Organization B is a member of a consortium whose IdP is supported by University C. To gain access to the SP, Char and Jen use their University digital credentials and Sue uses her consortium digital credentials.
2. **Multi-campus/consortium and single IdP**
   a. **Separate Licenses**
   Sue is a student at a multi-campus University. The university employs a single IdP to manage digital identities. Electronic resources are sometimes licensed by individual campus based on their respective curriculums. Sue is a student at campus A but is currently taking a online class at campus B. Sue must read several articles for the class at Campus B. One of the articles is available to JSTOR with the Campus B license. Even though Sue is registered as a student at campus A she is entitled to access the article at JSTOR because she is taking a class at campus B.
   b. **Multiple licenses with one vendor**
   Sam is a law student and Pete is a undergraduate at a university that employs a single IdP to manage digital identities. The law school licenses journal L with vendor Y specifically for the law school students, faculty and staff. The University has licensed journal Z, with vendor Y. Sam accessed an article in journal Z and proceeds to search the site for related content. He finds and accesses a related article in journal L. Pete accessed the same article in journal Z but when he searches for a related article there were no results from journal L.