NISO Webinar • February 11, 2009

Single Sign-On Authentication: Understanding the Pieces of the Puzzle

- Todd Carpenter, Managing Director, NISO
- Adam Chandler, Coordinator, Service Design Group, Digital Library and Information Technologies, Cornell University Library
- Steven T. Carmody, IT Architect, Computing and Information Services, Brown University
- Keith Dixon, Access & Identity Management, Eduserv
- David Orrell, Identity Systems Architect, Eduserv
- Lyn Norris, International Business Development, Eduserv
- Jerry Ward, ProQuest Platform Product Manager

NISO Webinar • February 11, 2009

Towards Horizontal Linking to Licensed Content

Adam Chandler
Cornell University Library

Single Sign-On Authentication: Understanding the Pieces of the Puzzle
NISO Webinar • February 11, 2009


Patrons are trying to break out of our vertical architecture

Google as a primary research tool

• Sufficing, when quality isn’t a concern
• Insufficiently aware of library e-resources
• Bad experiences with library e-resources

Chief inhibitors to success in using library resources

• Lack of awareness
• Difficulty navigating library website to locate appropriate e-resources
• Search catalog front and center, for articles

• Authentication barriers, especially considering limited access points

How students choose resources

• Library outreach
• Course instructor
• Brand awareness
• Google

What happens when Cornell patrons try to access our most heavily used licensed resources from Google?

"web of knowledge", google rank? 1

"factiva", google rank? 1
“firstsearch”, google rank? 1

“pubmed”, google rank? 1
Do patrons set their affiliation in Google Scholar?

90% of the requests to the Cornell link resolver from Google Scholar in January 2009 came from on campus, where IP-based affiliation happens automatically for the user.
towards ...
InCommon Library/Shibboleth Project Update

Steve Carmody
Brown University/Internet2

Goals for the Library/Shibboleth Project

Provide:

- Integrated access to licensed library resources regardless of user location
- Consistent user experience for authentication and redirects between sites
- Reduced maintenance overhead for librarians
- Reliable authentication for vendors

What is the Library/Shibboleth Project?

- Established 2007
- Six universities + Internet2
- Campus IT, Library IT, Librarians

Goals for the Library/Shibboleth Project

- Evaluate whether adding Shibboleth to the existing access control framework provides additional value to users and librarians
- Develop best practice recommendations
Approach Taken by the Library/ Shibboleth Project

- Identify user scenarios
  - On-campus
  - Off-campus
  - Library walk-in
- Explore how use cases change when Shibboleth is introduced
  - Policy
  - Business practice
  - Technology
- Identify and Test proposed solutions
- Document findings

What is Shibboleth?

- Open source, standards-based web single sign-on package (supports SAML v1.1, SAML v2)
- Supports the “Federated Identity” model
  - Identity Provider (IdP) authenticates the browser user, and provides Attribute Assertions describing the user
  - Service Provider (SP) validates the Assertions, makes an Access Control decision, and provides Resources
  - Each player identified by a unique entityID value
- Leverages local identity management system

What Does Shibboleth Provide?

- Enables access to both campus and external applications
- Protects users’ privacy
- Helps your service partners
- Plays well with others
- Adoption by 20+ other Higher Education/Research federations

A Typical User Session

- Access Application/Service Provider Site
- Identify Home Site
- Redirect to Home Site Shibboleth IdP
- Authenticate locally
- IdP determines which attributes to release
- Redirect back to Application, carrying Attribute Assertions
- SP site uses Assertions to determine access rights, and to personalize

Phase 1 - Accomplishments

- Identified use cases and current issues with accessing licensed electronic resources
- Enumerated business and technical issues
- Identified approaches to specific issues
- Component testing for individual situations, in standalone environments
- Recommend hybrid approach (proxy + Shibboleth)

Shibboleth + SSO enabled rewrite proxy

Benefits to users
- Single password for campus service and proxy access
- Single login for entire browser session
- No user-side configuration needed
- Integration with personalized vendor functionality

Benefits to librarians
- Reduced cost of support
- Less IP and proxy maintenance by accessing high-traffic resources via Shibboleth
- Permits rollout of Shibboleth-enabled resources while keeping user experience consistent

Benefits to vendors
- Authoritative validation
- Easier breach investigation
- No maintenance of password information

Benefit to library administration
- Central usage statistics (“foot traffic”)
Phase 2 Objectives

• Pilot functional testing, in a stepwise fashion, in production environments
• Enumerating implementation issues
• Identifying high-priority vendors
• Developing recommended standards for content providers
• Collaboration with other groups investigating federated access

Getting involved

• Informal
  • EZProxy users, use Shibboleth for EZProxy authentication
• Formal
  • Contact us
  • Steven_Carmody@brown.edu

More Information

• http://www.incommon.org/library

About Eduserv

A registered charity governed by trustees
- Dedicated to realising the benefits of IT for
  - Learners, researchers & institutions that serve them
- Driven by the needs of the community
  - Access and Identity Management (Athens/OpenAthens)
  - Web Solutions – Develop/host sites (Education/Public sector)
  - Licence Negotiation Services – Publisher and software
Tensions and Trust

Balance risks to access and user privacy with the usability of services and monitoring for management.

Many Publishers – Many Subscribers

Requires a framework of business relationships supported by standards and technology to be effective.

Technologies, Standards & Federations (2)

**Athens - a technology, services AND a “federation”**

- Established as the ‘standard’ for UK Universities, colleges and the NHS (UK National Health Service)
- Mediates a trusted relationship between Service Providers and their Subscribing Organisations
- NOW
  - users in 100 countries
  - Software AND Hosted Service options
  - OpenAthens provides Shibboleth support and access to UK federation for 350 UK HE/FE institutions
- Access to resources from around 180 leading service providers
- More than 10,000,000 authentications per month

Technologies, Standards & Federations (1)

- IP Authentication – A trusted “pipe”
  - Simplicity
  - No offsite access
  - No personalisation – so drives 2nd login
  - No fine-grained authorisation/diagnostics/statistics
- EZProxy – A trusted third-party “pipe”
  - Allows offsite access
  - BUT still
    - No personalisation – so drives 2nd login
    - No fine-grained authorisation

The challenge of accessing published resources has grown with the scale and complexity of the resources available.

Trust

Standards & Technologies

Usability and Deep Linking
Technologies, Standards & Federations

- **SAML – An OASIS Open Standard** - A language and protocol
  - “An XML-based architecture, framework and protocol for the secure exchange of security credentials between separate security domains.”
  - Works on a federated trust model - No managed service at the centre
- **Shibboleth – An Internet2 Project** - A technology ENABLER
  - A project that has managed the development of an architecture and a code package, running on a variety of systems
  - A technology that an organisation can use to authenticate and assert a user’s entitlement to access a service provider’s resource as part of an agreement between the organisation and the service provider.
- **Federations** are relationship ENABLERS
  - Organisations and service providers can reduce the cost of multiple, similar bi-lateral relationships by participating in federations that provide a shared legal framework within which relationships can be developed

Users, Identity and Usability

- **Consistency of experience**
  - Presentation standards
  - Usability/Personalisation vs. Identity Risk
    - Highly valued identity data (attributes) e.g., passport number, national insurance number vs. low-value identity data e.g., research interests, affiliations (?) etc.
    - Usability & Personalisation == Portable profile data?
      - spanning services (common presence)
      - transitioning affiliations (lifelong)
    - User-centric Identity Management (e.g., OpenID)
      - Enables users to control release of identity data
      - Users can release profile data in return for greater usability (consistency/more personalised services)
    - Resource Accessibility - e.g., “Deep linking”

Philips Research Library Project

**Requirements**
- Single-Sign-On solution
- Seamless linking to their journals
- Differential access for divisions
- Stats by division for apportioning costs
- Phase out their own proxy server
- Driving force – Jan van Nijnatten

**Solutions**
- Eduserv – Athens Service
- TDNet - ejournal manager

Usability Case Study: Philips

- Headquartered in the Netherlands,
- Employ 121,000 people in 60+ countries worldwide.
- Sales of EUR 26 billion in 2008
- Market leader in
  - cardiac care, acute care and home healthcare, energy efficient lighting solutions and new lighting applications
  - home electronics, especially TV

Proxy Server
Athens

Organisation

Internet

Vendor website

Firewall

Athens

User

usernames

Proxy server

Athens using Local Authentication

Organisation

Internet

Vendor website

Firewall

Athens

User

usernames

Proxy server

Active Directory

Vendor website

Firewall

Athens

User

usernames

Proxy server

Active Directory

Athens Local Authentication plus Proxy Server

Philips SSO Solution

Combination of EZproxy & Athens Local Authentication

- Athens – Local Authentication using Philips Research Active Directory
  - 47 resources, thousands of journals
    - 11 Athens compliant
    - Remainder delivered using Athens Managed Proxy Service
- EZproxy using Athens as authenticator
- Athens browser session cookies
- Allows any resource to be included in the ‘federation’

Authentication Points

Multiple authentication points, against different directories
Journal level links - examples

- Journals and articles referenced in a variety of ways:
  by ISSN, DOI, mnemonic, OpenURL, PMID
- http://gut.bmj.com/contents-by-date.0.dtl
- http://ageing.oxfordjournals.org/

Proxy journal links

Typically journal links include IP authentication

- Link resolvers can easily put the proxy prefix in

Journal Links with Athens authentication


Philips SSO plus seamless journal links

Created journal URL syntax for each vendor separately

- Incorporated into TDNet’s A to Z product
- BUT forced to proxy ScienceDirect
  - No journal links with Athens authentication
  - ScienceDirect journal links work, but Philips isn't eligible for a federation
- Philips rolling this out across their divisions this month

Next steps

Short-term
- Initiate/Support standardisation efforts
- Develop community approach
  - Build & publicise a Knowledge Base of Deep Links
  - Collate knowledge from Athens users
  - Encourage/cajole vendors into providing deep links with authentication

Medium/Long-term
- Drive standardisation to a conclusion

Summary

- Tensions & Trust
  - Usability vs. Privacy
- Technologies, Standards & Federations
  - IP Auth, EZProxy, Athens/OpenAthens, SAML/Shib
- Users, Identity & Usability
  - Consistency of User Experience
  - Usability/Personalisation vs. Privacy
  - Resource Accessibility eg. Deep Linking
- Usability – Philips and Deep Linking
SSO Authentication: Understanding the Pieces of the Puzzle.

Jerry Ward
ProQuest Platform Product Manager

Wednesday, February 11, 2009

Who am I?

• 13 years in Tech Support at ProQuest.
• Involved in solving authentication problems for customers.
• Now the Platform Manager for the ProQuest Platform.

View from “The Front Line”

• Support costs are huge.
• Staff at both the institution and the content provider get requests from end users having authentication problems – usually more than all others combined.
• Development cost are high for adopting each new feature that comes along, even if very few use it.
• Technology changes, and then what was working no longer does – Referring URL Yes! / Referring URL NO!
• We as a company have supported everything from individual system assigned usernames and passwords to Shibboleth.

The Problem

• People have so many account credentials they cannot keep track of them.
• Everything from trivial to critically important.
• Leads to frustration as they cannot remember what set of login credentials to use when challenged.
• Users just want access without problems.

Libraries = Starting Place

• Many users start their research at Google.
• Why – Not because it is the best resource, but because it is the easiest to enter.
• Google does not get them access to the high-quality resources libraries pay for.
• We need to remove the barriers to entry for the libraries’ electronic resources.
• If there is even the smallest hurdle, many will not even try to jump it.

What is Out There

• ID/Password
• Barcode
• Referring URL
• Embedded Token
• IP
• Athens
• Shibboleth
• LDAP
• OpenID
• Kerberos
Confusion

- We have found that even institutions have trouble keeping straight what authentication systems go to what.
- Legacy Systems, Registration, Financial …
- Cost in IT Resources – Libraries are often at the bottom when these resources are allocated.
- Then users may have access through different organizations – How to keep those straight?
- Users may not even recognize a portal that will get them in.
- Even more so now with Link Resolvers are directing you from one system to another one that has what you are looking for.

The Time Is Now

- Almost all problems can be solved with either a large amount of resources or in a way that is too complicated for the average user or both.
- However, with the changes in technology, this problem can now be solved with a reasonable effort and in a way that most people can use it.
- It is time for a common standard and a system that will benefit everyone – from the library to the content provider to the user.
- Just as OpenURL brought linking into common usage, so a standard SSO system will bring it into common usage.

Questions??

Questions?

All questions will be posted with presenter answers on the NISO website following the webinar:

www.niso.org/news/events/2009/authentication09

Thank You!

Thank you for joining us today. Please take a moment to fill out the brief online survey.

We look forward to hearing from you!