SUSHI IMPLEMENTATION: THE CLIENT AND SERVER EXPERIENCES

DEDICATED TO STANDARDS

EXTENDING AND PROMOTING THE USE OF OPENURL

ESTABLISHING SUGGESTED PRACTICES REGARDING SINGLE SIGN-ON
Establishing Suggested Practices Regarding Single Sign-On (ESPReSSO) Working Group

In 2009, NISO launched a new Chair’s Initiative—a project of the chair of NISO’s Board of Directors, focusing on a specific issue that would benefit from study and the development of a recommended practice or standard. The issue proposed by then Chair Oliver Pesch was perfecting a seamless, item-level linking through single sign-on authentication technologies in a networked information environment.

Accessing information in a networked environment has been a reality for most user communities for over a decade. With the advent of hosted, aggregated full-text databases and the proliferation of e-journals and e-books, research often takes a user to a number of different online hosts and platforms as part of a single transaction. When those information resources are commercial products, each platform requires the user to be authenticated and, as a result, that user may have a different identity on each platform. The problems caused by having to manage multiple identities have led to the development of so-called “Single Sign-On” (SSO) authentication technologies, including proprietary technologies such as Athens and formal open standards such as SAML (Security Assertion Markup Language). With these technologies, the user can access all compliant content platforms using the same identity. More importantly, these technologies have been designed so the user will encounter only one login event while traversing a multitude of in-sourced and out-sourced service providers.

Simplifying the user experience has become more important as organizations have outsourced more and more of their supporting business functions. Making the SSO environment work better (smarter) will certainly help increase the success of users getting to the content to which they are entitled; however, it is probably fair to say that the majority of content hosts are not compliant with one or more of the current SSO authentication technologies.

Library users are required to operate in an environment that includes a mix of authentication technologies with IP authentication being the most common. An effective solution needs to address this hybrid environment and, at the very least, take into consideration the needs of IP authentication and proxy servers, and how they interoperate with SSO authentication technologies.

The Challenges

This Working Group was primarily concerned with the situation where an organization (a company, a campus, a public library, etc.) acquires a license to access specific content and where the user is a member of the group authorized to access that content. This Working Group did not address the situation where an individual would obtain a license for personal use.

Authentication has become complex for several reasons:

- The Internet world has evolved to provide users with many more options. Users can follow different paths, traversing multiple websites, in order to enter a publisher’s site. The result is that users arrive at many different points on the publisher site. It has been difficult to create a consistent, coherent user experience amidst all this variety.
Users may experience multiple authentication mechanisms, depending on how they enter the publisher’s site. Sometimes, the user’s physical location could affect the browser flows and authentication mechanisms they see. Within the publisher site, the user might—in innocently—navigate from a public page to a protected page, and thus unwittingly trigger authentication.

Publishers generally have to present and support multiple authentication mechanisms. They have to construct and present a usable authentication GUI interface that somehow combines multiple methods into an interface that can be used successfully by people with a low familiarity with technical concepts.

Campuses have deployed various approaches to authentication over the years; some of them require users to be able to use, handle, and manipulate proxy-prefixed URLs that are incomprehensible to the average person.

Figure 1 illustrates the many ways that a user can potentially enter a publisher’s site.

Each of the following communities is affected in negative ways when confronted with today’s authentication environment:

Library Community
Patron demand for remote access to content via computer or mobile device has become the norm rather than the exception. Libraries must provide patrons with an efficient, seamless way to access content and to search across content from multiple sources without continually being challenged for credentials, or having to change the steps they follow as a function of their physical location.

Publisher Community
As licenses increase in their complexity, customers may participate in numerous agreements, allowing varying degrees of access at an institutional, consortial, departmental, or other level. Keeping track of which affiliated users have access to what content becomes more challenging all the time. At the same time, customer demands for privacy concerning their users’ personal details and online search behavior have grown at an
even quicker pace. Spurred to action by support for single sign-on amongst European federations, publishers and content providers have labored to meet the varying requirements, including certification, interface adaptation, required attributes, and more. Streamlining the process has become essential.

**End User Community**

Researchers and students have access to content through a variety of channels; however, if access is from outside of the university’s IP range, a multitude of usernames and passwords might be required. When seeking access to a secured resource, a researcher is unable to identify easily what authentication will be needed and whether the publisher/aggregator supports SSO. The researcher is often unable to navigate to the institutional logon page, identify the appropriate federation and institution, and, once authenticated, return to the secured resource without multiple disruptions for separate authentications. The various stages of this process are not generally identified and branded sufficiently so that the request for credentials is not misinterpreted as phishing or malware.

Variability in the user experience creates a high level of confusion, and results in users giving up rather than being able to complete their tasks. The high level of variability also creates a maintenance nightmare for publishers and user education challenges for libraries.

**eSPReSSO Recommendations**

The eSPReSSO Recommended Practice document will recommend practical solutions for improving the success of SSO authentication technologies in providing a seamless experience for the user. It further aims to promote the adoption of one or more of these solutions to make the access improvements a reality. This initiative does not invent any new technology or protocols for the recommendations. Rather, it has developed a set of best practice recommendations surrounding the use of existing technologies. These recommendations are intended to define a path forward from the current access control mechanisms—which are increasingly problematic—to the next-generation approaches that promise to be more secure, easier to manage, more flexible, and provide more functionality. Consequently, the recommendations describe a “hybrid” environment containing older authentication approaches that are being deprecated and newer approaches that are in the early stages of implementation.

The recommendations draw on several years of experience and a variety of approaches. The majority of the recommendations refer to the newer approaches to access control and are intended to provide a consistent user experience across multiple service provider sites. Many of the recommendations were called out in the JISC-sponsored focus group study for Project FLAME, published in August 2009. The eSPReSSO report builds on that study and presents a set of recommendations to both identity provider (IdP) and service provider (SP) sites. The recommendations specifically address typical browser flows, the sequence of pages presented to users, page layout, what information to include in each of those pages, consistent GUI elements, and additional features and functionality to provide users with added value.

The recommendations are intended to:

1. Provide users with a consistent experience across a multitude of sites and situations.
Reduce user confusion and aborted sessions during the discovery/login process by using a consistent set of visual elements as the user is transferred between sites in order to reinforce the “this is normal and expected” aspect of the experience.

Be straightforward and easy to implement for both IDP and SP sites.

Recommendations to publishers include the preferred location for login links and input boxes, standard approaches for guiding users to a desired authentication method, where local branding information could be inserted on a webpage, as well as approaches for handling automatic logins. Recommendations for campuses include strategic use of institutional and publisher branding and an institutional menu page that transfers the user to the “automatic login” endpoint at the SP.

Next steps
The Recommended Practice is expected to be issued prior to this article’s publication. A likely next step following the publication of the ESPReSSO recommendations is the creation of a standing committee to be tasked with outreach support and updating the guidelines and related resources as needed. Related resources include maintenance of a website containing ESPReSSO FAQs for publishers, libraries, and aggregators. Other possibilities include a step-by-step implementation guide, webinars during which SPs who are new to SSO may troubleshoot with SP technical experts, and assistance with federation contracts and correspondence. The recommendations and the additional resources will all be available from the ESPReSSO website. An e-mail interest group list is available for anyone who would like to follow the group’s work, comment on or ask questions about the recommended practice, or share SSO experiences with others on the list. doi:10.3789/isqv23n1.2011.09

HEATHER RULAND STAINES - heather.staines@springer.com - is Senior Manager eOperations at Springer Science + Business Media. HARRY KAPLANIAN - harry.kaplanian@serialssolutions.com - is Director of Research and Innovation at Serials Solutions. KRISTINE FERRY - kferry@uci.edu - is Director of Web Services at the University of California, Irvine Libraries.

ESPRESSO Working Group Members

Steven Carmody
Brown University (co-chair)
Frank Cervone
Purdue University Calumet
Adam Chandler
Cornell University Library
Pete Confetti
Credo Reference
Andy Dale
OCLC Online Computer Library Center
Kristine Ferry
University of California, Irvine
Andy Ingham
University of North Carolina Chapel Hill Libraries
Harry Kaplanian
Serials Solutions, Inc. (co-chair)
David Kennedy
Duke University
Ted Koppel
Auto-Graphics, Inc.
Ulrike Lengwenat
Springer
Peter Noerr
Muse Global, Inc.
Lyn Norris
Eduserv
Kishor Patel
ProQuest
Oliver Pesch
EBSCO Information Services
Heather Staines
Springer Science + Business Media
Pieter van Lierop
Infor Library and Information Solutions
Robert Walsh
EnvisionWare, Inc.
Foster Zhang
Johns Hopkins University

ESPRESSO Website
www.niso.org/workrooms/sso
ESPRESSO Interest Group list
www.niso.org/lists/ssoinfo
ESPRESSO Charge
www.niso.org/workrooms/sso/charge