



University of Southern California: Shibboleth and Pubcookie at USC- Authentication and Authorization for All

NSF Middleware Initiative (NMI) Integration Testbed Case Study Series

Series contact: Mary Fran Yafchak, Southeastern Universities Research Association,
maryfran@sura.org.

The NMI Integration Testbed Program provided practical evaluation of NMI components within the context of real projects and application scenarios from June 2002 through November 2004. During that time, NMI Testbed sites collectively submitted over 220 evaluation reports to middleware component developers as direct feedback into the NMI development cycle. Site representatives also actively inspired, promoted and facilitated the integration of middleware throughout their institutions.

The NMI Integration Testbed Case Study Series documents the most significant influences and outcomes of NMI Testbed sites' middleware integration efforts, highlighting intersections with established projects, application contexts and influences, drivers for innovation, decision points and challenges. Through this, the work of these pioneering institutions is captured to provide a breadth of insight and approaches for others to use towards successful middleware development and deployment.

This NMI Integration Testbed Case Study Series is sponsored by the National Science Foundation Middleware Initiative-Enterprise and Desktop Integration Technologies (NMI-EDIT) Consortium of EDUCAUSE, Internet2, and SURA. Additional support was provided by the National Science Foundation Cooperative Agreement NSF 02-028, ANI-0123937.

Copyright © 2004 University of Southern California. The University of Southern California permits use of this content for noncommercial purposes with proper attribution. All rights reserved.



NMI Components Highlighted in this Case Study

The NMI components discussed in this case study series encompass NMI Releases 1 through 4. Information about NMI Releases can be found at <http://nsf-middleware.org/>.

Pubcookie

Pubcookie is open source software that supports intra-institutional web initial sign-on.
Home site: <http://www.pubcookie.org/>

Shibboleth

The Shibboleth technology supports inter-institutional sharing of web-based resources subject to access controls.
Home site: <http://shibboleth.internet2.edu>



University of Southern California: Shibboleth and Pubcookie at USC - Authentication and Authorization for All

The University of Southern California (USC) participates in a host of collaborative projects with other institutions across the country, from the Southern California Earthquake Center (SCEC) to the Scholar's Portal for library research. In order to facilitate secure and stable inter-connectivity with these projects, the university had to find a technology that would enable users to connect with a low degree of technical difficulty, but a high level of confidence. To complicate matters, participants in these projects may not be members of the USC community, but will still need authorization to gain access to the systems and records in question.

To enhance their understanding and peer support for relevant middleware development and deployment, USC began collaborating in the summer of 2002 in the National Science Foundation's (NSF) Middleware Initiative (NMI) Integration Testbed¹, a program developed and managed by SURA (Southeastern Universities Research Association) on behalf of the NMI-EDIT Consortium². The NMI Integration Testbed provides participants with the opportunity to perform

"real life" evaluation and provide feedback on NMI middleware software, specifications, and services, to enhance the work of their faculty and researchers. The Information Services Division at USC has endeavored to involve as many departments as possible in using and evaluating middleware components, such as NMI-EDIT's [Shibboleth](#)³ and [Pubcookie](#)⁴, and GRIDS Center technologies. USC has leveraged this experience to provide identity management for the applications discussed above.

A Solution for Authorization

Shelley Henderson, the middleware project director at USC, knew about [Shibboleth](#), the NMI-EDIT Consortium's open-source, standards-based tool providing mechanisms for controlling access to web based resources, from its inception. Henderson was also the champion of the school's later participation in the NMI Integration Testbed. By working in the Testbed, she was able to track [Shibboleth](#) through NMI Releases as it moved from architecture to tangible software component, and pushed to get it installed on campus as soon as the released code base was stable. An initial test installation was done to determine local technical

¹The NMI Integration Testbed consists of eight universities participating in a closely coordinated effort to deploy and evaluate NMI technologies.

<http://www1.sura.org/3000/NMI-Testbed.html>

²The NMI-Enterprise and Desktop Integration Technologies Consortium: <http://www.nmi-edit.org/>

³Shibboleth information: <http://shibboleth.internet2.edu>

⁴Pubcookie information: <http://www.pubcookie.org/>



requirements and to verify whether suggested possible applications, such as InscriptiFact (an image database of inscriptions and artifacts), were actually feasible candidates for Shibboleth-enabling. With federations (such as InCommon⁵) in development, USC has successfully Shibboleth-enabled applications that depend solely on the school's own origin (thus a Shibboleth target doesn't need to be running at the other site). InscriptiFact was eventually disqualified under this criterion because of requirements for authentication and authorization of users from a wide variety of origins. However, implementation with other applications was successful early on, partly because they met this criterion.

Shibboleth is currently being employed in a demonstration of the ARL Scholars Portal⁶, as well as Napster and Blackboard, and could be used for Tenet/USCNet (see below) along with other projects (such as InscriptiFact, above) in the wings for future development. Tenet/USC was briefly considered as a Shibboleth application due to HIPAA requirements, but was disqualified under the same criterion as InscriptiFact – Tenet (the Tenet Healthcare Corporation, which owns USC Hospital) would need to provide an origin to authenticate and authorize against, which they do not have.

⁵ InCommon is a formal federation of organizations focused on creating a common framework for trust in support of research and education.

<http://www.incommonfederation.org/>

⁶ The ARL Scholar's Portal -

<http://www.arl.org/access/scholarsportal/> White paper includes Jerry Campbell (USC CIO and Head Librarian) <http://www.arl.org/access/scholarsportal/SPupdateMay04.html>

Additional multi-university grants and projects will be enabled more smoothly by Shibboleth, as researchers obtain authorization to share resources. Administrators also expect to use Shibboleth and other middleware programs to manage the school's email lists in the future. Shibboleth's authorization decisions will be based on the forthcoming USC Enterprise Directory system.

Linking Authentication and Authorization

In early 2001, as the University was researching the possible uses for Shibboleth to bridge a variety of local authentication mechanisms, a related NMI middleware technology called Pubcookie became available in the authentication space. Pubcookie provides the web-based initial sign-on (WebISO) authentication service Shibboleth depends on.

After evaluating Pubcookie within the NMI Integration Testbed, the USC Information Services Division (ISD) decided to deploy Pubcookie for web-based authentications, for which they were receiving an increasing number of requests. Pubcookie allows web-based applications to authenticate using the University's already installed and enterprise-wide Kerberos system, which is synchronized with the University's UNIX login IDs and passwords. This then allows application developers to concentrate on their application problem, and permits ISD to maintain control over vital security infrastructure.



At one point, [Pubcookie](#) was also considered as a possible authentication mechanism for web-based email. However, it was never used as such. There was a strong desire by the University community for web-based email and they decided to incorporate a web-based solution in the move from classic Unix-based /var/mail to a central mail server. The University now has a centralized mail server in place running SunOne (formerly, iPlanet).

To evaluate the performance and utility of [Pubcookie](#), ISD installed it to protect their intranet in early 2003. The web development group reviewed the first draft of the client installation documentation, submitting feedback through their NMI Integration Testbed evaluation reports, and modifications were included in the next release. [Pubcookie](#) has been running on the ISD intranet for over a year now, with few obstacles.

Following the intranet implementation, USC created a website, <http://www.usc.edu/authx>, which includes instructions on how to set up [Pubcookie](#) client software on Wintel servers, plus a zipped version of the USC-localized [Pubcookie](#) client software. In addition, ISD includes [Pubcookie](#) as a normal part of its support for ISD-maintained Solaris boxes. It is now so straightforward to set up a [Pubcookie](#)-protected website at USC that students and faculty alike have used it to shield their personal websites.

[Pubcookie](#) is also now used for the nagios (an open-source, network monitoring program) status display for the HPC Linux cluster, replacing a live-status display based on Ganglia. Even though Windows users must do the work of installing [Pubcookie](#) themselves (because University policy does not allow ISD to do desktop support), users have found it very easy to get [Pubcookie](#) running and protecting their websites. UNIX users on ISD-supported hosts are even more fortunate, because a [Pubcookie](#) installation is included in the support package.

Other schools at the University, such as the theater school and the business school, are also using [Pubcookie](#) for various applications. Use is spreading slowly, by word-of-mouth, to those who need authentication services. However, the program will eventually take over for many independent systems that are currently performing their own authentication scripts. The majority of the installation, testing and coding work to date has been done by John Mullins, the technical lead, also known as USC's "Pubcookie Man."

Future Directions in Authentication and Authorization

As the use of [Pubcookie](#) spreads across campus, users are requesting functionality that the software cannot provide. While [Pubcookie](#) has served well as an authentication service, it was not designed



to do user authorization, which was a reason to install **Shibboleth**. Phil Dibowitz, the technical lead for USC projects related to **Shibboleth**, has found **Shibboleth** documentation consistently good and the underlying software base dependable. He expects that, at some point, **Shibboleth** will provide its own authentication mechanism that will make the current use of **Pubcookie** redundant. If **Shibboleth's** target installation can be made as easy as the current installation of **Pubcookie**, its authorization mechanisms will provide the extended functionality that current web-based application developers are requesting and ISD would push for the installation of **Shibboleth** targets rather than **Pubcookie**.

As of the fall semester 2004, version 1.1 of the **Shibboleth** origin is deployed and working properly. ISD is not planning to upgrade the origin until **Shibboleth** v1.3 is available. The initial target installation was also version 1.1. However, due to the inability of v1.1 targets to meet specific requirements for the Napster and USC Portal projects, it was deemed necessary to move to v1.2 for those targets. For the Napster project, technical lead Phil Dibowitz built and deployed an operational **Shibboleth** v1.2 target because of the inability of the **Shibboleth** v1.1 target, on the advice of **Shibboleth** Project technical personnel, to meet the requirements of a production installation. **Shibboleth** v1.1 targets do not support lazy sessions, a feature required for the USC portal project. **Shibboleth** v1.2 targets *do* support lazy sessions, so it was

decided to move to v1.2. (In a “lazy session,” the system defers the creation of a **Shibboleth** session until the application determines it is needed, allowing a single URL to provide access to both open and protected content.⁷ In other words, it now allows for guest authorization to access certain systems.)

Shibboleth Applications

Shibboleth is beginning to thrive at USC with new and developing production-quality applications. USC-Napster is operational for the fall semester of 2004, and the university is now running demonstration project for the Scholar’s Portal. The USC Portal will be fully operational for the spring 2005 semester. Some testing has been done with database programs such as Inscriptifact (for Middle-eastern artifacts and inscriptions) and **Shibboleth** authorization has been successfully combined with the Blackboard course management system, which will be put into use as soon as the “shibbolized” version of Blackboard is stable. Below is additional detail on deployment and use of each of these.

Napster

USC is one of eight universities currently working with the Napster music download service to provide legal music downloads for students. Other institutions with similar agreements include Pennsylvania State University, Cornell University, and

⁷ Shibboleth 1.2 functionality:
<http://shibboleth.internet2.edu/release/Shib-1.2-features.html>



George Washington University. For an annual fee of \$20, students are granted unlimited listening to Napster's library of over 800,000 songs (they still have to pay the \$.99 fee for permanent song downloads, however). For the Napster installation, the company's technical team wanted to use **Shibboleth** for authorization. USC has set up a Shibboleth-enabled web portal page⁸ for students, available for the fall semester 2004.

The Scholars Portal

The Scholar's Portal⁹ is a web presence for electronic or online resources that are owned by the members of the Association of Research Libraries (ARL). The ARL wants its members to be able to share all of the available resources of its member libraries. The Scholar's Portal is basically a search aggregator, which allows searching throughout licensed electronic resources, eliminating the need to do multiple searches. Scholar's Portal provides access to licensed electronic resources (e.g., Lexis-Nexis) and so requires that ISD know about and explicitly permit access.

The Scholar's Portal proof of concept site was unveiled at USC during the summer of 2004, and is undergoing testing. It is using USC's **Shibboleth** 1.1 origin for authorization, and a

Shibboleth 1.2 target. The Scholar's Portal will also make use of "lazy sessions" for guest authorization. Other institutional members of ARL, including Arizona State University, University of Arizona, Iowa State University, and the University of Utah have also launched the Scholars Portal search capability on their campuses. However, USC is the first to actively engage in the project using **Shibboleth** authorization.

Blackboard

Blackboard is the main course management system employed at USC, and can be Shibboleth-enabled "out of the box" (1). USC is working with Blackboard to have a Shibboleth-enabled version of Blackboard's software available for student use in time for the spring 2005 semester.

USC Portal

The full functionality of USC Portal¹⁰ is expected to be available for the spring 2005 semester. The Portal will be a personalized information point for students, faculty and staff, with password-protected access. The USC Portal will provide single-sign-on to Blackboard, web-based email, Oasis (student information system), and web registration. It will incorporate news, announcements, notification channels, a briefcase, calendaring, bookmarks, and logging. Authorization processes for the USC Portal will be through

⁸ <http://www.usc.edu/isd/napster/>

⁹ <http://www.arl.org/access/scholarsportal>

¹⁰ <http://my.usc.edu>



Shibboleth, and developers have set up “lazy sessions” to be used with version 1.2.

More Information

For more information about [Shibboleth](#) and [Pubcookie](#) use for authentication and authorization at USC, contact Shelley Henderson at shelley@usc.edu.

References

(1) Blackboard Announces Internet2 Shibboleth Compatibility- 4/9/2003 , Washington, DC - Blackboard Inc.
<http://www.blackboard.com/about/press/prview.htm?id=510431>

Information in this paper is based on interviews during August 9-11, 2004 with the following individuals:

- Shelley Henderson, Middleware lead, ISD
- John Mullins, Project Lead, Pubcookie
- Phil Dibowitz, Project Lead, Shibboleth.



