Against the Grain

Volume 24 | Issue 3 Article 40

June 2012

Standards Column

Todd Carpenter
NISO, tcarpenter@niso.com

Recommended Citation
Carpenter, Todd (2012) "Standards Column," *Against the Grain*: Vol. 24: Iss. 3, Article 40.
DOI: https://doi.org/10.7771/2380-176X.6299

Standards Column — Need a shot of ESPRESSO? Improving the Single Sign on Experience and Other Identity Management Issues

by **Todd Carpenter** (Managing Director, NISO, One North Charles Street, Suite 1905, Baltimore, MD 21201; Phone: 301-654-2512; Fax: 410-685-5278) <tcarpenter@niso.org> *www.niso.org*

Managing your credentials has never been more complicated. Years ago, a person usually had a driver's license, perhaps a passport, perhaps a library card, a corporate or student ID, and a ring full of keys. OK, perhaps a bit more than that. But today, the number of credentials that one must manage has grown exponentially. This is largely true because of the numerous login and password combinations and other credentials necessary to navigate our online environment. And this problem is exacerbated if you move from institution to institution, have multiple organization affiliations, or regular accesses electronic resources with authentication requirements.

There are a variety of types of identity management tools related to your online interactions. One definition of identity management is the active management of your personal information online — akin to ensuring no one is saying negative things about you online. Another definition would be the curation of the creative output you have published or otherwise released online. Still another definition would be the management of the credentials you might have to access content, portals, or other online resources. All three of these different approaches are interrelated. Successfully addressing any one of these applications will have implications on the others. Fortunately, there is a variety of work underway to improve identity management and access control.

Over the years, content providers learned that usernames and passwords simply did not scale for centrally-managed institutional access systems. For end-users, password requirements to prevent hacking have grown to the point that passwords are incapable of being remembered, and managing them next to impossible without a management tool — unfortunately, often a cheat-sheet taped to the computer screen serves this purpose. The most-often implemented solution to simplify access control for users, content providers, and licensing institutions has been IP address authentication. While the IP address access control is convenient, it increasingly became unwieldy as remote working and then mobile computing exploded, and as licenses became more complex with different privileges for different sub-populations of the same institution. It also creates significant security and unauthorized access issues. The response was often the implementation of proxy servers to authenticate users. Management of these proxy servers can be very resource-intensive and may not work correctly with Websites using complex scripting or deep links.

It is within the context of this hybrid environment of authentication that **NISO's** Establishing Suggested Practices Single Sign On (ESPReSSO) project was conceived. The goal of the project was to create a **NISO** Recommended Practice that would improve single-sign-on (SSO) authentication to achieve seamless item-level linking in a networked information environment. The resulting ESPReSSO Recommended Practice (available for free download at *http://www.niso.org/workrooms/sso/*) identifies a path toward phasing out old methods of userid/password, IP authentication, and proxy servers in favor of an SSO experience across a set of distributed service providers. ESPReSSO does not put forward a new authentication structure or technology but rather promotes a path forward to broad-based implementation of Security Assertion Markup Language (SAML)-based authentication, such as Shibboleth. Recognizing that the transition will not occur overnight, the ESPReSSO Working Group identified a number of practices that can be implemented right away to improve user interaction, interface elements, and standard approaches for guiding the user to the desired content. Additionally, the recommendations address how to make appropriate trade-offs between advanced functionality (e.g., stored search sessions) and privacy and the use of authentication with the new Web-scale discovery environments in libraries.

Over the past six months, there was advancement on several other identification fronts in our community. First, development of centralized unique identification systems for scholarly (and broader) identity management was completed for both the International Standard Name Identifier (ISNI) and the Open Researcher and Contributor ID (ORCID). Both systems launched roughly on schedule in the first quarter of 2012.

The ISNI system and infrastructure were created to implement the International Standard Name Identifier standard (ISO 27729), which was published in March of this year. ISNI was created to unambiguously identify the public persona of parties through a network of registration agencies, each representing an industry segment that will manage specific metadata about the particular party as it relates to that industry. For example, the recording industry will manage identities and metadata specific to recording artists, musicians, etc. The collected metadata will be collated at the ISNI central registry where the ID assignment and disambiguation work will take place. The initial data included in the system is derived from the Virtual International Authority File (VIAF) managed by **OCLC** in cooperation with more than 20 national libraries. Use of VIAF and other databases of the founding members of the **ISNI International Agency** allowed the pre-assignment of close to one million identifiers. Because of its diversity, the engagement from a broad swath of content creator communities, the distributed nature of the system, and the seeding of the ISNI system with over 24 million contributors' references, the ISNI system is poised to improve discovery and rights management for content creators.

NISO's Institutional Identifier (I^2) Working Group that was working simultaneous with the ISNI standard's development for a solution to unique identification of institutions in the e-resource supply chain, saw an opportunity to extend the use of the ISNI to institutional identification, rather than creating yet another identifier for this purpose. Following a number of discussions in 2011 between the I^2 Working Group and the **ISNI International Agency**, agreement was reached to use the ISNI and its database system for institutional identification. At least one registration agency will be appointed later this year by the **ISNI International Agency** to assign ISNIs to institutions and collect the relevant metadata to be added to the ISNI master database.

Within the scholarly and academic communities, there has been a great deal of momentum building behind the Open Researcher and Contributor ID (ORCID) system. More than 300 organizations have committed to participate in ORCID, and more than 50 are contributing financially to the project. ORCID is building a system to support user-authenticated data on individual researchers. ORCID recently announced the appointment of **Laure Haake** to lead the organization as Executive Director. Beta testing of APIs and data interchange with the ORCID system is underway, with a full launch of the user ID system in the fall of 2012. There have been conversations among the principles about ways in which ORCID and ISNI can interoperate. At the moment, there is commitment from ORCID to use the same numbering structure, with a range of ORCID IDs being reserved from the ISNI system.

While a number of issues related to identity management remain to be solved, it is refreshing to report the significant progress our community has made over the past year. In all likelihood, these systems will gain rapid adoption in our community since the problems that they address are areas of significant pain in our community. We are finally in a place where standards are in place and technologies sufficiently mature to be broadly applied to identity management issues. Now that the systems are in place (or shortly will be), the critical activities related to education, training, and adoption of these standards and recommended practices must begin in earnest. After all, standards that are released, but not implemented, are not terribly useful to anyone.