INFORMATION STANDARDS QUARTERLY
FALL 2014 | VOL 26 | ISSUE 3 | ISSN 1041-0031

ISQ

TOPIC

IDENTITY MANAGEMENT

PRIVACY BY DESIGN AND THE ONLINE LIBRARY

FROM THE LIBRARY OF CONGRESS TO THE LIBRARY OF ME

THE INTENTION PUBLISHING ECONOMY: WHEN PATRONS TAKE CHARGE

A JSON-BASED IDENTITY PROTOCOL SUITE

NISO
How the information world CONNECTS

NISO RECOMMENDED PRACTICE:

Establishing Suggested Practices Regarding Single Sign-On (ESPReSSO)

Authentication has become complex and the older authentication methods are not manageable for either the content provider or the library. NISO's ESPReSSO Recommended Practice (NISO RP-11-2011) give guidance to Service Providers (SPs), Licensee Organizations (LOs), and Identity Providers (IdPs) on how to provide users with a consistent experience across a multitude of sites and situations, reducing user confusion and aborted sessions during the discovery/login process.

AMONG THE RECOMMENDATIONS ARE:

- SPs and LOs move quickly to reduce reliance on **IP-based access control.**
- SPs and LOs deprecate userids/passwords validated at the service provider site and use **standards-based federated authentication.**
- SPs adopt **standard placement/wording of the login link** on all the public pages on their site.
- IdPs create a **consistent experience** as the user moves from SP to IdP to SP.
- SP and IdP web designers insert **branding** at appropriate places in the flow to provide visual feedback that the flow is progressing as expected.
- SPs offer a **single URL point of access** for IP authentication and federated login.

The ESPReSSO Recommended Practice is available for free download from the NISO website at:

www.niso.org/workrooms/sso

espresso

ISQ

FALL 2014 | VOL 26 | ISSUE 3 | ISSN 1041-0031

NISO
How the information world CONNECTS

INFORMATION STANDARDS QUARTERLY (ISQ) is a publication by the National Information Standards Organization (NISO). ISQ is NISO's print and electronic magazine for communicating standards-based technology and best practices in library, publishing, and information technology, particularly where these three areas overlap. ISQ reports on the progress of active developments and also on implementations, case studies, and best practices that show potentially replicable efforts.

CONTENTS

NISO UPCOMING 2014 EDUCATIONAL EVENTS

www.niso.org/news/events

NOVEMBER

12 Keyword Search = "Improve Discovery Systems" (*Webinar*)

19 Can't We All Work Together? Interoperability & Systems Integration (*Virtual Conference*)

DECEMBER

3 Connecting the Library to the Wider World: Successful Implementations of Linked Data *(NISO/NFAIS Virtual Conference)*

NISO Two-Part Webinar: Sustainable Information

10 **Part 1:** Digital Preservation for Text

17 **Part 2:** Digital Preservation of Audio-Visual Content

Webinar Subscription Package Discounts

» Buy 5 NISO webinars & get 4 free

» Buy 9 NISO webinars & get 5 free – attend the whole series

» Buy 4 NISO virtual conferences & get 2 free

NISO Open Teleconferences

Join us each month for NISO's Open Teleconferences—an ongoing series of calls held on the second Monday of each month as a way to keep the community informed of NISO's activities. The call is free.

Andy Dale

LETTER FROM **THE GUEST CONTENT EDITOR**

I am honored and humbled to have been asked to guest edit this issue of *Information Standards Quarterly* on Identity Management. I have been involved in the evolution and application of identity standards for many years and am thrilled to have been able to bring authors from very different disciplines together to contribute to this issue. I hope you find this as informative, insightful, and entertaining as I do.

The same way as Bring Your Own Device (BYOD) has been reshaping the face of institutional computing, Bring Your Own Identity (BYOI) will be equally impactful. It is probable that BYOI may even helps us overcome some of the unresolved issues of BYOD. Devices are often used as a proxy for Identity but they are a poor proxy at best. The articles in this issue start to show how the emerging identity management standards can be leveraged to solve long-standing problems.

Dan Blum's piece on *Privacy by Design* establishes some of the core patterns for applying the latest standards to build systems that leverage the new standards. Dan introduces concrete ways that systems can be designed and built that solve existing problems while increasing personal privacy, assurance, and control.

Don Hamparian gives us a glimpse into what is happening at OCLC, an organization enabling controlled access to licensed content on a global scale. OCLC is a true leader in this space having built a SAML-based federation with 23,000 institutional partners acting as Identity Providers. Don's work at OCLC is a great example of what can be done today bringing these standards together with a strong institutional desire to engage with end users in a respectful and privacy-protecting way.

Doc Searls, one of the thought leaders in the identity standards space paints a picture of a world where the emerging standards have become commonplace. Doc's vision helped create the bi-annual Internet Identity Workshop (IIW), the conference where the cutting edge of internet identity innovation is formed. Doc has also been one of the primary shepherds for the advancement of Vendor Relationship Management (VRM), a user centric alternative to Customer Relationship Management (CRM).

Finally, **Mike Jones's** piece introduces us to the richness of the JSON-based identity protocol suite that has evolved from protocols such as OpenID and OAuth. While these protocols originated in and emerged from the social networking space they have been rapidly adopted (for standards ☺). They have evolved to support a wider range of use cases with higher levels of assurance and can support transactions of higher value and regulatory compliance needs.

It may seem remiss not to mention the SAML-based protocol stack[1] in an issue about identity management. We decided that rather than repeating recently covered territory we would refer you to the NISO Establishing Suggested Practices Regarding Single Sign-On (ESPReSSO)[2] recommended practice, which has been covered previously in this publication[3] (see also inside front cover in this issue). SAML and the Shibboleth[4] implementation of SAML are widely adopted in institutional identity management.

Interestingly, leading commercial products such as Microsoft's Azure Active Directory and Ping Identity's Ping Federate product have been extending their support for the JSON-based identity protocol suite alongside their support for SAML.

I hope that a journey through this issue of ISQ will leave you not only better informed about the standards that are evolving in the Identity Management space but also help you understand the intention behind those standards and the promise that they represent. doi: 10.3789/isqv26no3.2014.01

All the best,

Andy Dale | *CTO of Respect Network Corp.*

[1] SAML. https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=security

[2] ESPReSSO. http://www.niso.org/workrooms/sso

[3] Staines, Heather Ruland, Harry Kaplanian, and Kristine Ferry. "Establishing Suggested Practices Regarding Single Sign On (ESPReSSO) Working Group." *Information Standards Quarterly*, 2011 Winter, 23(1):34-37. http://www.niso.org/publications/isq/2011/v23no1/staines/

[4] Shibboleth. https://shibboleth.net/

DAN BLUM

PRIVACY BY DESIGN

AND THE ONLINE LIBRARY ENVIRONMENT

This paper focuses on ways that libraries can incorporate advanced identity management concepts within the Privacy By Design framework to meet their needs as they continue their transition from the brick, mortar, and paper era to an era of mixed physical and digital content. In order to add value over and above what researchers can find with search engines and freely available content on the Internet, libraries must excel at supporting both ordinary knowledge seekers and academic researchers in fulfilling their content- and collaboration-related needs. Increasingly, libraries must support a seamless, personalized, and collaborative experience for diverse audiences across the full lifecycle from content discovery to content delivery while at the same time protecting patrons' privacy and intellectual property prerogatives.

Changing Business Trends

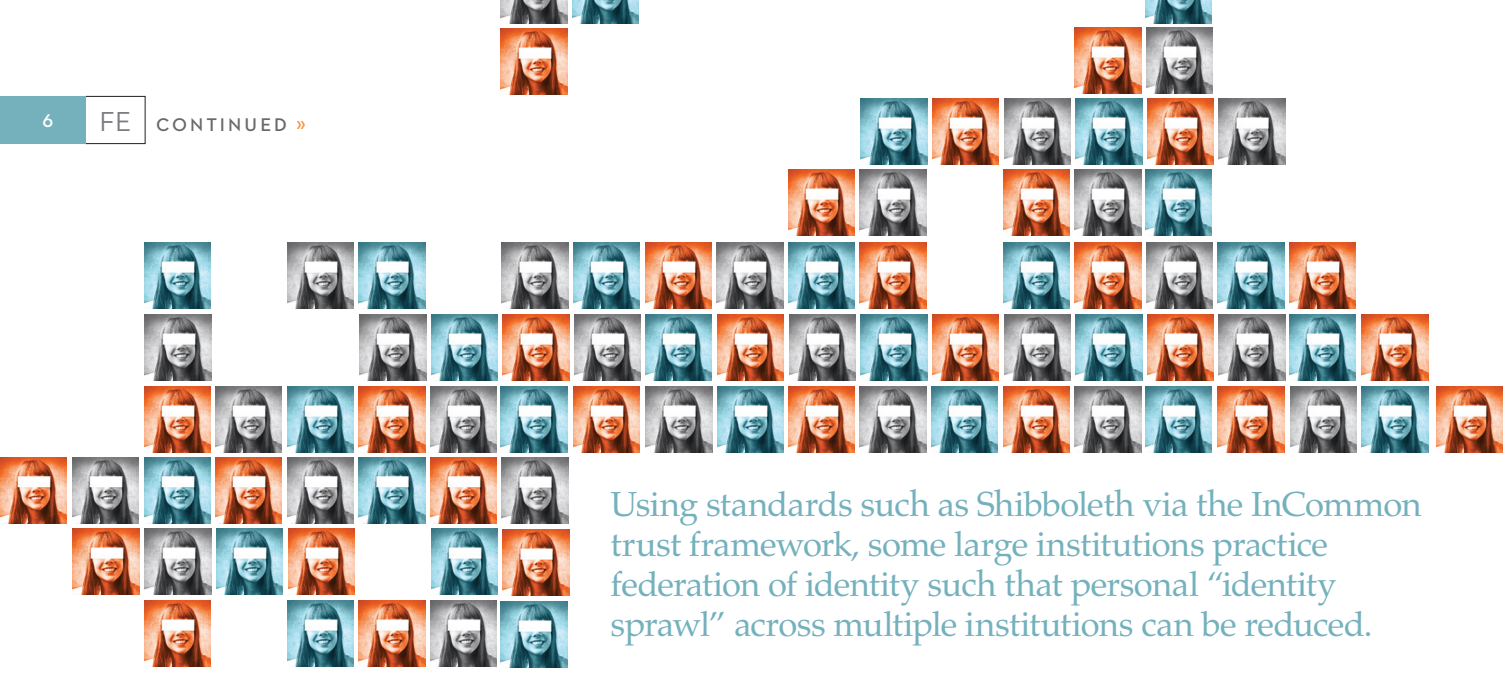
Like many industry segments, higher education and public libraries face a business imperative to support more complex online use cases for patrons and partners. Each library patron has a unique constellation of needs and relationships. Faculty, staff, students, alumni, and even "walk-ins" (or visitors) may be associated with multiple borrowing or authorizing institutions. Each partner library, research institution, business, or content provider may also have different entitlements and licensing or other business practices that must be respected.

With the requirement to differentiate from, or add value to, the ocean of free Internet content, libraries must support value-added services or content that are not provided freely to anonymous users. As research and collaboration enablers, they must support these services from discovery to delivery, in some cases providing a level of full-text search without "giving away the farm" to subscribing institutions, customers, or partners.

At the far end of the spectrum for business value and disruption, many businesses, and even individuals, may simultaneously become both consumers and providers of premium or restricted content in the growing "bring your own cloud" and "bring your own identity" environments. Thus, the library of the future could intermediate research and collaboration exchanges between complex fabrics of lenders, personal clouds, content providers, and businesses. To do so will depend on meeting requirements for richer identity and entitlement information interchange between actors in various use cases.

Each library patron has a unique constellation of needs and relationships.

CONTINUED »



Using standards such as Shibboleth via the InCommon trust framework, some large institutions practice federation of identity such that personal "identity sprawl" across multiple institutions can be reduced.

An increasingly diverse and inter-dependent library environment will bring new challenges as well. Often, information providers sharing their premium content will expect to get personal information on patrons, or to deliver advertising to patrons as a quid pro quo. These advertising endeavors could in turn ensnare libraries in a web of dubious relationships, as the author described happening to other online services in his article *Dark Lords of the Internet*.

Regulatory Risk

Juxtaposed against the growing business need for rich identity and entitlement interchange is the continuing movement for privacy regulation. This trend is creating tremendous tension between the advertising technology model ("ad-tech model") for online service delivery and the law. Libraries are already governed by the Family Educational Rights and Privacy Act (FERPA) and similar regulations. To the extent they operate internationally, engage non-U.S. patrons, and store personal records of students or patrons, libraries may also fall under a growing wave of international regulations.

In 2014, revelations of pervasive public and private surveillance by Edward Snowden, the CBS show *60 Minutes – The Data Brokers*, and other sources outraged public opinion, pouring gasoline on the regulatory fire. Even in the U.S., the Federal Trade Commission (FTC) and privacy consumer activist groups now actively hunt for privacy terms abusers. Libraries that try to expand identity data interchange and retention without a strong leavening of Privacy By Design will do so at increased risk.

Other Risks

Libraries face more than just regulatory risk as both their public and academic industry sub-segments frequently come under cyber-surveillance or cyber-attack. Even libraries that don't deliberately abuse privacy may be held liable for negligence if they:

- allow patrons to be hacked from infected library networks or computers;
- fail to assure the confidentiality and integrity of licensed content against the efforts of malicious patrons, fraudsters, and hackers;
- leak too much personal information on patrons to unscrupulous private data brokers in a harmful manner or on a large scale; or
- cooperate with or allow unwarranted law enforcement or other government searches of patron data and activity.

The endless inventiveness of cybercriminals and scammers is already taking its toll on the industry as seen in reports of Russian websites trafficking in user ids and passwords granting access to library proxy servers.

Identity and Privacy Issues for Libraries

Libraries have multiple issues with operational inefficiency, fraud, and regulatory risk arising from shortfalls in existing identity and privacy-related practices. Some issues—such as resale of proxy user ids, or of an entire patron database and subsequent release of passwords by cybercriminals—can arise for a single institution. Other issues occur in the context of multi-library interactions and the over-sharing of patron information.

In theory under the inter-library loan protocols, lending institutions should not have to obtain patron information—dealing with the patron should be the responsibility of the borrowing institution holding the patron relationship. Using standards such as Shibboleth via the InCommon trust framework, some large institutions practice federation of identity such that personal "identity sprawl" across multiple institutions can be reduced. Often, however, practice lags theory. Proxies may not be well integrated with identity systems providing a single campus id. Many institutions don't participate in the InCommon federation or have use cases—such as the need to support direct end user interaction with non-library content providers—not readily supported by the standards.

Basic business practices may be only marginally compliant with FERPA. Although FERPA provides a substantial loophole where institutions can designate large amounts of personal information as "directory information" to support over-sharing and over-storing arrangements, they often don't provide sufficient transparency to patrons or the ability for patrons to opt out of integration with third-party services that could result in information leakage to data brokers, advertisers, or worse. Should the regulatory climate tighten, even large institutions such as Harvard University could come under pressure to narrow their definition of "directory common elements" and provide greater permissioning granularity to patrons.

Technology Trends

Shibboleth and the Security Assertion Markup Language (SAML) on which it is based are showing their age. While some provisions exist for handling attribute assertions as well as authentication, a new crop of "claims-based identity standards" are emerging. Implementing these standards to provide claims-based access control may help libraries reduce their privacy compliance risks from identity sprawl and over-sharing. For example, a library could reply with a "U.S. citizen" token or "age over 18" token rather than personally-identifying information about the patron to enable certain authorization use cases.

While necessary, current claims-based identity standards won't be sufficient. Unfortunately, the OAuth 1.0 and 2.0 specifications on which most of the standards are based have numerous security weaknesses, and when used in practice by providers such as Facebook, Google, and Microsoft, tend towards the over-sharing and overly-permissive registration practices characteristic of the model rather than a Privacy By Design-based approach.

Standards groups in the Internet Engineering Task Force (IETF) are working to remedy some of these flaws by adding proof of possession, JavaScript Object Notation (JSON) cryptographic tokens, and new dynamic registration specifications, but it may take years before major online providers driving the identity technology space implement them. Thus, although emerging pre-standards such as OpenID Connect and User Managed Access (UMA) may provide some basic claims-based plumbing, more assurance is needed on the security robustness and trustworthiness of the underlying OAuth protocol they currently rely on.

Some in the industry, such as members of the FIDO Alliance, envision that ubiquitous mobile devices never far from the users' hands may provide better identity assurance. They hope to leverage native device capabilities such as Apple's iTouch to use the mobile device as a strong identity token for online interactions. But skepticism abounds that interoperability will be universally attained, or that sub-$500 commodity devices floating around in users' purses and pockets can gain the hoped-for assurance.

Bring your own identity (BYOI) is emerging not only from the FIDO Alliance, but from a new category of personal information management (PIM) products and services. PIM product categories, such as personal data stores and user-centric personal clouds, are often premised on the individual, rather than some centralized cloud service, controlling both storage and sharing of personal data in keeping with strict privacy principles.

CONTINUED »

Some in the industry, such as members of the FIDO Alliance, envision that ubiquitous mobile devices never far from the users' hands may provide better identity assurance. They hope to leverage native device capabilities such as Apple's iTouch to use the mobile device as a strong identity token for online interactions.

BYOI solutions are sometimes criticized for only providing self-asserted identity, as if organization-asserted identity was always much more trustworthy. This misses the larger point that, whatever the original source of identity information, the risks of impersonation and fraud will always be with us, especially as the information drifts through chains of intermediaries that take it further and further from the source. Protocols alone cannot solve this problem of assurance; what's needed are trust frameworks and/or reputation systems that operate at the legal and social layer of the relationships of online communities relying on them.

Having trust frameworks (or agreements that enable participants who share or accept identity credentials—and identity, authorization or reputation claims—to operate under well-defined policies) is especially important when a strong requirement for privacy is added to traditional security objectives such as confidentiality and integrity. Some providers in the personal information management category are banding together around user-centric trust frameworks such as Respect Network. In these frameworks, privacy is the default setting, informed consent is required for all permissions, pseudonymity is an option, and the right to be forgotten is also specified.

How Online Libraries Can Apply the Seven Principles of Privacy By Design

Privacy by Design is an approach to IT systems development that takes privacy into account throughout the whole engineering process. The concept is analogous to "safety by design," i.e., to take human safety into account in a well defined manner. The concept is believed to have originated in a 1995 report by Canada's Information and Privacy Commissioner and Netherlands' Registratiekamer on *Privacy-Enhancing Technologies*. Dr. Ann Cavoukian, the former Information and Privacy Commissioner, Ontario, Canada, has promoted the concept of Privacy by Design since the late 1990s and manages a website with the name.

The seven foundational principles of Privacy by Design, which have been translated into over 35 languages, are:

1. *Proactive* not Reactive; *Preventative* not Remedial
2. Privacy as the *Default Setting*
3. Privacy *Embedded* into Design
4. Full Functionality – *Positive-Sum*, not Zero-Sum
5. End-to-End Security – *Full Lifecycle Protection*
6. *Visibility and Transparency* – Keep it Open
7. *Respect* for User Privacy – Keep it *User-Centric*

The following sections consider each foundation principle from the library industry perspective, building on Ann Cavoukian's and Drummond Reed's paper *Big Privacy: Bridging Big Data and the Personal Data Ecosystem Through Privacy by Design*.

PROACTIVE NOT REACTIVE; PREVENTATIVE NOT REMEDIAL

"The *Privacy by Design* approach is characterized by proactive rather than reactive measures. It anticipates and prevents privacy-invasive events before they happen. PbD does not wait for privacy risks to materialize, nor does it offer remedies for resolving privacy infractions once they have occurred—it aims to prevent them from occurring. In short, *Privacy by Design* comes before the fact, not after."

Libraries, and online businesses in general, have many opportunities to deploy proactive Privacy by Design solutions. That is because both advertising-based and non advertising-based systems have tended greatly towards centralized models of personal information storage. In this model, the organization with access to all their users' personal information sets all the terms and conditions of use. Centralized systems create, in effect, a single information silo that cuts individuals off from meaningfully participating in a market "based on a resource that they themselves (mostly) produce, namely their personal information." Privacy risks abound under such a model, not only because the data controllers have incentives to exploit personal information without regard to the subjects' preferences, but also because risk aggregates in the large centralized systems, and the more of them there are, the more identity information sprawls.

Solutions that decentralize control of personal information either to the individuals themselves (e.g., personal clouds) or at least to the organizations that have a closer relationship to the individual (e.g., borrowing libraries rather than lending libraries) may prevent many privacy risks from arising by putting people more in control of their information. They can also improve operational efficiency and assurance by moving the authoritative source for data closer to the individual, thus improving its quality and accuracy.

Every library, patron, and partner has its own unique constellation of relationships and entitlements. Library use cases are becoming more complex to address enhanced research and collaboration functionality enabling everything from discovery to delivery of a mixed universe of free and restricted content. Thus, the library community will need a mix of centralized, decentralized, and hybrid

identity topologies. Different topologies will favor different technologies falling broadly into the federated identity, claims-based access control, and BYOI technology categories deployed in a proactive, Privacy by Design manner. As the breadth of the communities grows and the use cases and privacy challenges become more advanced, trust frameworks and semantic authorization standards will also be required.

PRIVACY AS THE DEFAULT SETTING

"*Privacy by Design* seeks to deliver the maximum degree of privacy by ensuring that personal data is automatically protected in any given IT system or business practice. If an individual does nothing, their privacy still remains intact. No action is required on the part of the individual to protect their privacy—it is built into the system, by default."

Today, large online content and service providers replicate the personal information they've collected in duplicative, centralized databases. They then seek to monetize this information through data sharing arrangements for advertising. Privacy is not the default; instead it is obscured under the cover of complex privacy policies. While the requirement for privacy policies was intended by regulators to promote openness and greater transparency of an organization's processing of personal information, most in fact do precisely the opposite with long, difficult to understand legalese, which the user is required to accept as is or not use the service.

As libraries seek to expand research and collaboration services to patrons, they run the risk of being drawn into relationships with content providers that participate more heavily in the ad-tech economy and become tainted by association. To avoid such situations from occurring, cooperative library industry trust frameworks that are user-centric should be developed to control the web of relationships underpinning services. Such frameworks should ensure that privacy is the default setting and that all sharing of personal information is by permission only.

A trust framework legally binds *all* members of a trust community—both individuals and organizations—to a set of business, legal, or operational policies, as a condition of membership. For example, the Respect Trust Framework is a user-centric trust framework that sets down global terms and conditions for interacting with personal information in a manner that respects the privacy of individuals, with strong assurances of security. Libraries could participate in this trust framework or develop something similar for themselves. They could also strengthen privacy provisions for themselves as a sub-community of the InCommon trust framework.

Privacy is not the default; instead it is obscured under the cover of complex privacy policies.

PRIVACY EMBEDDED INTO DESIGN

"*Privacy by Design* is embedded into the design and architecture of IT systems and business practices. It is not bolted on as an add-on, after-the-fact. The result is that privacy becomes an essential component of the core functionality being delivered. Privacy is integral to the system, without diminishing functionality."

Libraries can embed privacy into design by:

- Moving to decentralized or federated architectures that minimize the collection of personal information from patrons
- Establishing network-wide trust frameworks so that information is shared only with privacy as the default and standards exist for de-identification of data required for analytics
- Using generalized roles (such as "student", "faculty", "staff", "visitor", "librarian") rather than identifiers or groups for authorization
- Using claims tokens, such as "over 18" or "U.S. citizen", rather than revealing private personal attributes
- Using pseudonymous identifiers for patrons

CONTINUED »

FULL FUNCTIONALITY – POSITIVE-SUM, NOT ZERO-SUM

"*Privacy by Design* seeks to accommodate all legitimate interests and objectives in a positive-sum "win-win" manner, not through a dated, zero-sum approach, where unnecessary trade-offs are made. *Privacy by Design* avoids the pretense of false dichotomies, such as privacy vs. security, demonstrating that it is indeed possible to have both."

A 2012 study by Edelman Digital found that "seven in ten people globally are more concerned about data security and privacy than they were five years ago, and a full 68% believe that consumers have lost control over how online personal information is shared and used by companies."

Privacy by Design advocates have been saying for years that privacy is good for business. When customers are knowledgeable about and fully involved in decisions about sharing of their personal data, they will have more confidence and trust and be more willing to share their personal information with libraries. This information can, in turn, be shared by permission—often in a de-identified manner—to personalize services both from the core library networks and from private sector partners. By providing de-identified patron analytics, libraries can, for example:

- Optimize acquisitions and collections management
- Incentivize content holders to make information more available
- Personalize content for different classes of patrons

By maintaining a strong reputation for integrity and privacy, academic and public libraries can protect or even expand their "market share" versus "freemium" information-based products and services on the Internet.

END-TO-END SECURITY – FULL LIFECYCLE PROTECTION

"*Privacy by Design*, having been embedded into the system prior to the first element of information being collected, extends security throughout the entire lifecycle of the data involved. This ensures that all data is securely retained, and then securely destroyed at the end of the process, in a timely fashion. Thus, Privacy by Design ensures cradle to grave, secure lifecycle management of information, end-to-end."

Through federated identity systems and claims-based access control, libraries can improve identity assurance overall. That is because institutions will put more effort into maintaining accurate information or protecting credentials for an identity that's relied on for single sign-on (such as a campus id) than for a one-off proxy service account. Alternatively, user-centric federations—such as those enabling personal cloud networks or BYOI—apply protection at the interface of the patron or partner. The patron will keep his or her own data accurate, both as the first to know of most changes and for self-protection.

However, such security measures become more complex and harder to manage as more parties are involved, such as multiple libraries and content providers. Federated identity systems through trust frameworks are again a solution to consider when data is shared among multiple stakeholders.

Personal information has a lifecycle, just like records, and must be destroyed on a timely basis in a secure and privacy-protective manner. Personal information should also not be replicated in multiple databases to avoid the existence of excessive copies, which might not get destroyed simultaneously. In the BYOI model, the authoritative source for private information is an individual's personal cloud, and a "subscription" model can be used to provide others with access. The individual retains control over when to delete data or turn off access.

VISIBILITY AND TRANSPARENCY – KEEP IT OPEN

"*Privacy by Design* seeks to assure all stakeholders that whatever the business practice or technology involved, it is in fact operating according to the stated promises and objectives, subject to independent verification. Its component parts and operations remain visible and transparent, to users and providers alike. Remember—trust but verify!"

The only way that users will have a real sense of control over their private information is with full transparency and understanding of how their personal data will be accessed, used, and shared by anyone who is party to it. As previously noted, a user-centric trust framework is the recommended method for such transparency and understanding. Because their terms and conditions are publicly reviewed and published and all members agree to follow them, trust networks can establish a community's best practices for privacy. Inter-library and third-party audits are one method of verifying and enforcing the trust's policies are being followed.

RESPECT FOR USER PRIVACY – KEEP IT USER-CENTRIC

"*Privacy by Design* requires architects and operators to keep the interests of the individual uppermost by offering such measures as strong privacy defaults, appropriate notice, and empowering user-friendly options....At its core, respecting the user means that, when designing or deploying an information system, the individual's privacy rights and interests are accommodated right from the outset. User-centricity is anticipating and designing in a person's privacy perceptions, needs, requirements, and default settings. It means putting the interests, needs, and expectations of people first, not those of the organization or its staff. Empowering people to play active roles in the management of their personal data helps to mitigate abuses and misuses."

Libraries also can adopt user-centricity as an operating principle. For various use cases they can offer users the convenience and control of BYOI (or a secure institutional identity), the protection of a user-centric trust framework, the option to use either pseudonymous or public identifiers, and the ability to share personal data under contracts that bind relying parties to de-identify the data.

Conclusion

The library industry, in seeking to become a network of scholarship, research, collaboration, and knowledge amidst oceans of uncurated Internet information, should adopt Privacy By Design into its core guidelines. Not only will Privacy by Design improve compliance postures, it can also be good for growing the evolving roles of libraries in information discovery and delivery. By taking a proactive approach to preventing privacy infractions, setting privacy as the default, and maintaining transparent, user-centric identity and privacy policies, libraries can find positive-sum solutions for participating institutions, partners, and patrons.

| FE | doi: 10.3789/isqv26no3.2014.02

DAN BLUM (dan@respectnetwork.net) is Chief Security and Privacy Architect with Respect Network and author of the blog Security Architect (http://security-architect.blogspot.com/). He is dedicated to addressing security and identity management issues from the enterprise, individual, and social perspectives.

RELEVANT LINKS

Blum, Dan. "Dark Lords of the Internet." ***Security Architect*** **[blog], June 9, 2014.**
http://security-architect.blogspot.com/2014/06/dark-lords-of-internet.html

Cavoukian, Ann, and Drummond Reed. ***Big Privacy: Bridging Big Data and the Personal Data Ecosystem Through Privacy by Design*****. Ontario: Information and Privacy Commissioner Ontario, Canada, December 2013.**
http://www.privacybydesign.ca/index.php/paper/big-privacy/

"The Data Brokers." ***60 Minutes*****. CBS, March 10, 2014.**
https://www.youtube.com/watch?v=_Cty7ctycsI

Family Educational Rights and Privacy Act (FERPA)
http://www2.ed.gov/policy/gen/guid/fpco/ferpa/

FIDO Alliance
https://fidoalliance.org/

Harvard University Common FERPA Directory Elements
http://security.harvard.edu/files/it-security-new/files/ferpa_directory_common_elements.pdf

InCommon Identity Assurance Assessment Trust Framework
http://www.incommon.org/docs/assurance/IAAF.pdf

The JavaScript Object Notation (JSON) Data Interchange Format
http://tools.ietf.org/html/rfc7159

The OAuth 2.0 Authorization Framework
http://tools.ietf.org/html/rfc6749

OpenID Connect
http://openid.net/connect/

Privacy & Security: The New Drivers of Brand, Reputation and Action**. Edelman Digital, 2012.**
http://www.edelmandigital.com/2012/04/05/privacy-security-the-new-drivers-of-brand-reputation-and-action/

Privacy By Design
http://www.privacybydesign.ca/

Privacy-Enhancing Technologies: The Path to Anonymity. **Information and Privacy Commissioner, Ontario, Canada and Registratiekamer, The Netherlands, August 1, 1995.**
Vol. 1: http://www.ipc.on.ca/English/Resources/Discussion-Papers/Discussion-Papers-Summary/?id=329
Vol. 2: http://www.ipc.on.ca/English/Resources/Discussion-Papers/Discussion-Papers-Summary/?id=242

Respect Network
https://www.respectnetwork.com/

Respect Trust Framework
http://openidentityexchange.org/trust-frameworks/respect-trust-framework/

Security Assertion Markup Language (SAML) specifications
http://saml.xml.org/saml-specifications

Shibboleth
http://shibboleth.net/

User-Managed Access (UMA) Profile of OAuth 2.0
http://docs.kantarainitiative.org/uma/draft-uma-core.html

IP [IN PRACTICE]

Don Hamparian

From the Library of Congress to the Library of Me

DON HAMPARIAN

OCLC is a worldwide library membership organization that helps libraries work together to connect people and information more efficiently. Founded in 1967 by a small group of library leaders, this non-profit cooperative now consists of thousands of libraries across the globe who actively participate in finding practical solutions for reducing information costs. OCLC's diverse library membership also works to explore trends that shape the future of libraries; to share data, work, and resources; and to magnify the impact of libraries worldwide.

Researchers, students, and other information seekers use our services to obtain abstracts and bibliographic and full-text information. OCLC and its member libraries cooperatively produce and maintain WorldCat®, the world's largest library catalog.

OCLC offers a host of bibliographic services for management and discovery of library collections. Many of our services are hosted at OCLC data centers for our institutions.

The focus of this article is OCLC's Identity Management services and vision and their place in the evolving role of OCLC services in the library community.

The Evolving Role of OCLC Services in the Library Community

Over the years, OCLC's services have been evolving in a variety of ways. A significant part of this evolution is the increasing involvement of the library patron and community as direct users of our services. Today, many of our services include patron self-service functionality, which involves a much larger community of users than even a few years ago. This evolution parallels the library's increasing role as a community hub—a non-partisan place to gather, meet, and exchange ideas and information. OCLC provides services that recognize this community-focused role of libraries. Our Identity Management infrastructure must keep up with this direction.

OCLC's Position of Trust in the Library Community

OCLC is a member-funded and member-governed not-for-profit organization. As such, we are uniquely positioned in the library community to provide identity services and to protect user information consistent with libraries' expectations. OCLC does not resell library user data or have a business model that depends on licensing or sharing this data.

As the range and reach of our services has grown, so has the emphasis on protecting users' privacy. This is a core ethic in the library community: the stewardship of user-related information that allows users to consume library services knowing that their privacy is respected and protected.

We run our Identity Management infrastructure in four data centers across the globe in order to segregate our identity data by region. Our data loading, reporting, and management processes are built to maintain this data segregation.

E-Content: Discovery to Delivery and OCLC's Vision of Identity Management

One of the primary use cases involving library users is the "Discovery to Delivery" workflow. In years past, this workflow involved searching the card catalog at the library and finding a book on the shelf or working with library staff to request the book from another library. Today, this workflow is handled mostly on users' computing devices and involves discovering an item via a variety of discovery websites (including the local library, OCLC, and many others) and then requesting the item for delivery. A large proportion of the "delivered" items are e-content objects from various publishers and aggregators. Delivering e-content has spawned a variety of tools and infrastructure, including link resolvers, federations, and groups; access and proxy software; and a myriad of administration screens for library staff to enter access information.

This process is frustrating for both library staff who manage the infrastructure and for the end users who can't easily access the materials they want. There are many steps, screens, challenges for credentials, and opportunities for something to go wrong. Usually, the authentication and authorization process uses IP address authentication, which is perceived as easy to administer but has a variety of security and usage limitations.

Related to the areas of access control and identity management, the predominant route to remote access of licensed e-content is through proxy servers. OCLC's EZproxy is one of the leading proxy servers used for this purpose.

Once all the administration and configuration is done, this environment works effectively. However, it still has some limitations, especially with broadband video and e-book borrowing management. Proxying increases network bandwidth consumption and often cannot provide the content provider with sufficient identity information to completely automate the workflow (such as for e-book borrowing).

CONTINUED »

We believe we can help libraries take the next step by building virtual communities relevant to the populations they serve.

OCLC's Identity Management Infrastructure and Vision

OCLC's infrastructure is a Shibboleth-compliant facility that provides unique Identity Providers (IdP) for every institution that consumes our WorldShare services. To date, we have configured about 23,000 IdPs for our institutions. We also provide interoperability with external, non-OCLC service providers and support institutions that wish to use their own IdP instead of OCLC's.

We run our Identity Management infrastructure in four data centers across the globe in order to segregate our identity data by region. Our data loading, reporting, and management processes are built to maintain this data segregation.

Our vision for Identity Management is to "lower the barrier of access to content and services while protecting licensed content and user privacy." We are accomplishing this vision by implementing the following:

1. **A standards-based interoperable infrastructure**
   Our infrastructure is natively a SAML 2.0 infrastructure with interoperability support with existing Shibboleth-based federations. Today we support operating with external institution-based Identity Provider and Service Provider components. We also support SAML 2.0 compliant Central Authentication Service (CAS) Identity Providers and can access institution LDAP or Active Directory servers as an alternative user/password database to our own.
2. **Single sign-on between OCLC services and institution facilities**
   Our infrastructure supports single sign-on with CAS and Shibboleth components. We also provide this support with our integration with LDAP and Active Directory since Service Providers see a standard Shibboleth Identity Provider with our integration.
3. **Integration points between e-content management and access control**
   This area remains to be significantly built out. Today, we integrate with EZproxy and OCLC's discovery services, but need to expand this integration to e-content providers and aggregators. This area will be our focus in the next few years.
4. **Identity management infrastructure for libraries who don't have the technical expertise to build it themselves**
   As noted, we have provisioned approximately 23,000 Identity Providers as part of our initial institution activation work. These Identity Providers are used for providing access to a variety of our services. By default, these Identity Providers start with identities defined for library staff. When a library uses WorldShare Circulation services, we also load all patron identities into our system unless the institution is using their own Identity Provider. We are considering offering other services to populate the Identity provider so that institutions can use them with both OCLC and non-OCLC service providers.
5. **A global solution compliant with regional laws and library expectations of privacy**
   We have to accommodate expectations of privacy from both legal and library perspectives. In both of these cases, the expectation and requirements of privacy vary by region. In the case of library expectations of privacy, these expectations can also vary by the type of library (for example, public, academic, school). Our implementation is built to provide strict segregation and protection of data by region and institution.

Solving the E-Content Access Problem

Solving the e-content access problem requires a reduction in the management/administration overhead required to provide access, the development of a standard method to provide appropriate identity data to e-content providers, and a reduction in the number of login challenges and authentication credentials the user needs to enter or remember. We believe that using a SAML-based infrastructure, such as Shibboleth, is a leading way to reduce our dependence on IP proxying and to provide true interoperability between libraries, content providers, and identity providers (such as OCLC). However, technology is only part of this solution. There are legal, cultural, and regional challenges to solving this problem. Also, we need to provide a solution for both browser and non-browser (mobile application) environments.

Using Identity Management to Build the Library Community

Libraries are natural organizations to build region-based communities. They are already popular gathering spots for people in the community and provide a non-partisan setting for community groups to gather. We believe we can help libraries take the next step by building virtual communities relevant to the populations they serve. In order to do this, Identity Management services can be used to determine that the community members are in fact affiliated with the library or the local region. This is a logical extension to the Identity Management services that OCLC provides.

Conclusion

Identity Management infrastructure has grown and evolved so far that the next generation of e-content access can be defined and implemented. The technology is mature and in wide use in academic institutions. Our remaining technical challenge is providing hosted and deployed solutions that are practical for smaller academic institutions and public libraries that don't have the technical support that larger academic institutions have. It is vital that our solution extends across all library types and sizes and can be easily implemented by both small and large content providers.

Technology is only part of the solution. No one organization will be able to completely solve the e-content access problem. We also have to continue to build the partnerships and trust between the institutions, identity providers, and content providers. Importantly, we have to extend this trust and technical services to public libraries and smaller academic institutions. These institutions don't have the legal and technical support required to participate in today's Identity Federations.

Libraries are natural organizations to build region-based communities. They are already popular gathering spots for people in the community and provide a non-partisan setting for community groups to gather.

Is a SAML-based infrastructure a cost-effective and easier to manage alternative to IP authentication, proxy, and multiple sets of credentials required to access e-content? We know that a SAML-based identity management infrastructure will provide more flexible and granular access to content, the ability to implement additional e-content based borrowing services, and allow widespread use of broadband content. Our challenge is to provide a set of affordable solutions that can be implemented by all ranges of libraries, institutions, and content providers. We believe our community is ready to meet that challenge.

| IP | doi: 10.3789/isqv26no3.2014.03

DON HAMPARIAN (hamparid@oclc.org) is Sr. Product Manager Identity Management at OCLC.

RELEVANT LINKS

OCLC
http://www.oclc.org/

EZproxy
http://www.oclc.org/en-US/ezproxy.html

Security Assertion Markup Language (SAML) v2.0
https://www.oasis-open.org/standards#samlv2.0

Shibboleth
http://shibboleth.net/

WorldCat
http://www.oclc.org/en-US/worldcat.html

WorldShare
http://www.oclc.org/en-US/worldshare.html

OP [OPINION]

A judgement formed about something;
a personal view, attitude, or appraisal

Doc Searls

DOC SEARLS

The Intention Publishing Economy: When Patrons Take Charge

Our editor has asked me to "imagine a world where identity management has fully evolved to serve the individual researcher's needs—a world where discovery to delivery of licensed content is a smooth and sane experience." Tall order, but he caught me at a good time; because, after many years of looking, I can now see a path to that future—one that ends with the *Internet of Things*, which is still almost pure buzz, as shown in Figure 1.

Amidst this early buzz, one finds two default assumptions about the Internet of Things. One is that to be "smart" things need embedded intelligence. The other is that the parties most responsible for smart things are their makers. Both are wrong.

Anything, literally, can be on the Internet. Your furniture, for example. Or your books. Or the magazine you are reading right now. All a thing needs is a unique identifier and standard ways that identifier can be understood and put to use.

So let's say a thing's identity is revealed through a QR code. (It just needs to be readable. For our purposes a QR code will do.) If you scan that code with your phone (or any device), it should be able to tell you what you need to know about the thing to which the code is affixed. For example, who owns it and what usage rights go along with it.

The thing telling you what you need to know is a *pico*, or *persistent compute object*. Phil Windley, Ph.D., who coined the term (and open source software to go with it), describes a pico as "a small, general-purpose, online computer." Picos can be anywhere on the Internet, and act as peers to other entities (e.g., companies, people, things, or even concepts) on the Internet regardless of size. Picos run programs and store data on behalf of the entities they represent. And picos create active, event-based channels with other picos to form a relationship network. Collections of picos, acting under the authority of their owners, can model the relationships and interactions between entities in the physical world. Everything in the world can have a pico. (To illustrate how this works, Dr. Windley even gave a pico to a pothole on his street.)

So let's talk about picos for books. In the long run, every book should come with its own pico, but for now let's imagine giving picos to every book you own. There will be easy ways to do this eventually (and an array of service businesses helping customers do that), but for now let's say you can do it yourself by sticking a QR code on the back corner of each book and scanning it with a reader that also picks up the ISBN number. The output of your scanning app can be programmed to route to another app made just for creating and managing picos. All your

books' picos will go in the personal cloud (itself a pico) where you keep everything that's yours in the Internet of Things (including permissions for use, set by you and/or the holders of copyrights). Anybody who later scans the code on one of your books can know it's yours—plus whatever else you and other rights holders choose to reveal.

A book with a pico can have relationships with its owner, publisher, seller, borrowers, other books, the movie that was made from it, or anything else that makes sense. The nature of these relationships is contextual and each enriches the book in some way by placing it in an important context. Programs running on the book's pico manage these relationships. For example, a "who's borrowed me" program could help the book (and its owner) keep track of who has read or borrowed the book, comments they had, or the book's current physical location.

Now let's say you donate your books to a library. When you do that, you also transfer the ownership of those books' picos. Then, when somebody scans the QR code on the same book, they'll see that the library now owns it—and also see the library's and the rights holders' permissions for using the book.

CONTINUED »

Collections of picos, acting under the authority of their owners, can model the relationships and interactions between entities in the physical world. Everything in the world can have a pico.

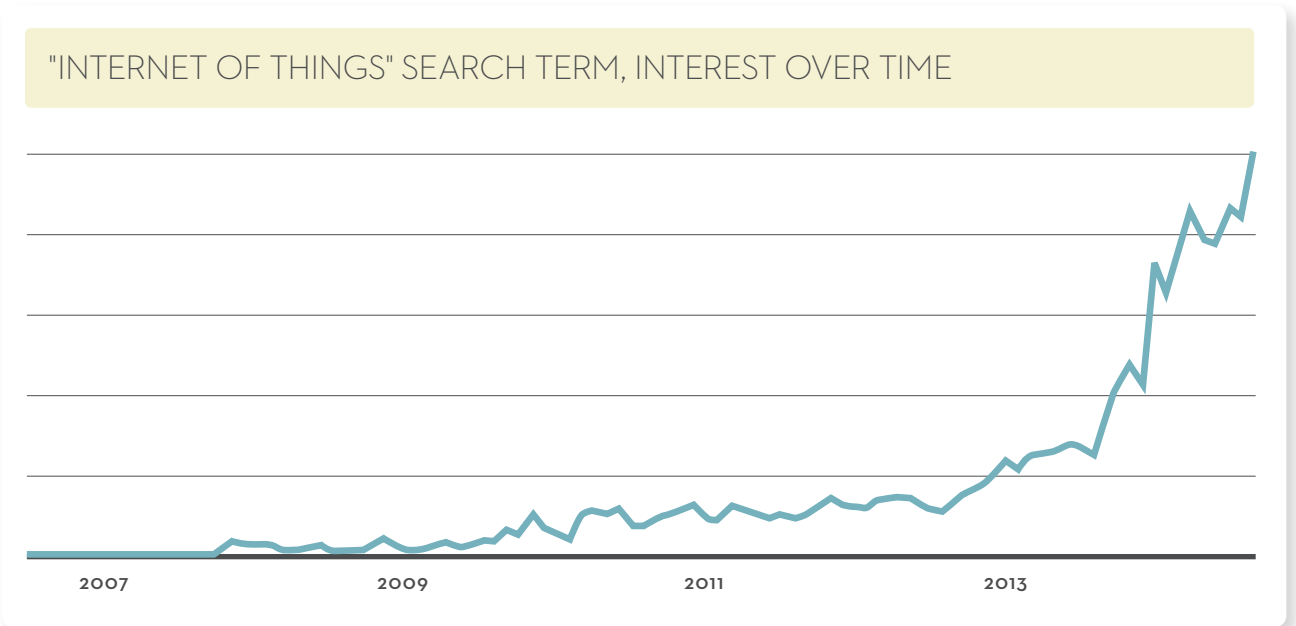


Figure 1: "Buzz" for Internet of Things

(Source: Google Trends, September 11, 2014. http://www.google.com/trends/explore#q=%22Internet%20of%20Things%22&cmpt=q)

"The goal of XDI is to enable data from any data source to be identified, described, linked, authorized, and synchronized using a standard semantic graph model, format, and protocol, so that data sharing can become as interoperable as HTML and HTTP have made content sharing."

And now let's say the contents of the book are available for scholarly use, online. You, as a researcher, should be able to discover and use that content, easily, and in permitted ways. This is only possible if there are standards governing all this, and they are widely adopted. This is what I expect to see happen with XDI, for eXtensible Data Interchange, which is already part of the spec for picos. According to the XDI Technical Committee at OASIS (a standards organization), "The goal of XDI is to enable data from any data source to be identified, described, linked, authorized, and synchronized using a standard semantic graph model, format, and protocol, so that data sharing can become as interoperable as HTML and HTTP have made content sharing."

A key word is *authorized*. XDI has a feature called *link contracts*, which bind usage to permissions. According to Wikipedia, "Link contracts are themselves XDI documents (which may be contained in other XDI documents) that enable control over the authority, security, privacy, and rights of shared data to be expressed in a standard machine-readable format and understood by any XDI endpoint."

I don't know any other standard that points more clearly in the direction we all want.

Many companies are starting to adopt and deploy XDI, mostly in what's becoming known as the "personal cloud" space (where, among other things, you control your own identifiers and manage relationships with other entities in the world). But it is still very early. There is no telling how fast or well developments will follow the path I've outlined here; but I'm encouraged by what I've seen so far. If you want to see more, follow along at ProjectVRM, which fosters this kind of work.

| OP | doi: 10.3789/isqv26no3.2014.04

DOC SEARLS (dsearls@cyber.law.harvard.edu) runs ProjectVRM at the Harvard's Berkman Center for Internet and Society, and is author of *The Intention Economy: When Customers Take Charge* (Harvard Business Review Press, 2012) and co-author of *The Cluetrain Manifesto* (Basic Books, 2000, 2010).

RELEVANT LINKS

OASIS XRI Data Interchange (XDI) Technical Committee
https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=xdi

ProjectVRM
http://projectvrm.org

Windley, Phil. "Fundamental Features of Persistent Compute Objects." *Technometria*, October 7, 2013.
http://www.windley.com/archives/2013/10/fundamental_features_of_persistent_compute_objects.shtml

Windley, Phil. "Personal Clouds as General Purpose Computers." *Technometria*, April 2, 2012.
http://www.windley.com/archives/2012/04/personal_clouds_as_general_purpose_computers.shtml

Windley, Phil. "Potholes and Picos." *Technometria*, April 9, 2013.
http://www.windley.com/archives/2013/04/pot_holes_and_picos.shtml

XDI. From Wikipedia, the free encyclopedia
http://en.wikipedia.org/wiki/XDI

SP [SPOTLIGHT]

Michael B. Jones

MICHAEL B. JONES

A JSON-Based Identity Protocol Suite

Achieving interoperable digital identity systems requires agreement on data representations and protocols among the participants. While there are several suites of successful interoperable identity data representations and protocols, including Kerberos,[1] X.509,[2] SAML 2.0,[3] WS-*,[4, 5, 6] and OpenID 2.0,[7] they have used data representations that have limited or no support in browsers, mobile devices, and modern Web development environments, such as ASN.1,[8] XML,[9] or custom data representations.

A security token is a cryptographically secured set of statements made by an issuer about a subject that can be used by the intended recipient to make trust decisions about the subject.

A new set of open digital identity standards have emerged that utilize JSON[10] data representations and simple REST-based[11] communication patterns. These protocols and data formats are intentionally designed to be easy to use in browsers, mobile devices, and modern Web development environments, which typically include native JSON support. This paper surveys a number of these open JSON-based digital identity protocols and discusses how they are being used to provide practical interoperable digital identity solutions.

THE EMERGING JSON-BASED IDENTITY PROTOCOL SUITE

This section provides an overview of a set of open, JavaScript Object Notation (JSON)-based digital identity protocols that are being collaboratively developed by members of the identity community. These protocols are designed to work together to enable open, interoperable, claims-based identity, authentication, and authorization services to be built for the Web.

JSON Web Token, Signature, Encryption, Key, and Algorithms Specifications

The ability to produce signed and optionally encrypted security tokens containing claims is fundamental to interoperable identity protocols. A security token is a cryptographically secured set of statements made by an issuer about a subject that can be used by the intended recipient to make trust decisions about the subject. Claims are the individual statements in the security token about the subject made by the issuer. This family of JSON-based specifications meets this need.

CONTINUED »

JSON Web Token (JWT)

A JSON Web Token (JWT)[12] is a means of representing claims to be transferred between two parties. The claims in a JWT are encoded as a JSON object that is digitally signed using JSON Web Signature (JWS)[13] and optionally encrypted using JSON Web Encryption (JWE).[14] Using a JWT enables the issuer of a token to make statements about the subject of the token to an intended audience in a way receivers can verify that they were made by the issuer. This capability is fundamental to digital identity systems. For instance, OpenID Connect[15] uses a JWT issued by the identity provider, whose audience is the relying party, to make authoritative claims that a particular user (the subject of the JWT) has logged in at the identity provider.

This specification was developed collaboratively based upon inputs from a number of independently developed precursor JSON token, signing, and encryption specifications. Over a dozen independent and interoperable implementations of JWTs are known to exist at this point—many of them in production use—including by Microsoft, Google, Salesforce, Deutsche Telekom, and Mozilla. The IETF OAuth Working Group[16] has requested publication of JWT as a Request for Comment (RFC)—an IETF standard.

The suggested pronunciation of JWT is the same as the English word "jot."

JSON Web Signature (JWS)

JSON Web Signature (JWS) is a means of representing signed content using JSON data structures. Complementary encryption capabilities are described in the closely related JSON Web Encryption (JWE) specification. For instance, the JSON Web Token (JWT) specification uses JWS for the issuer to sign JWTs.

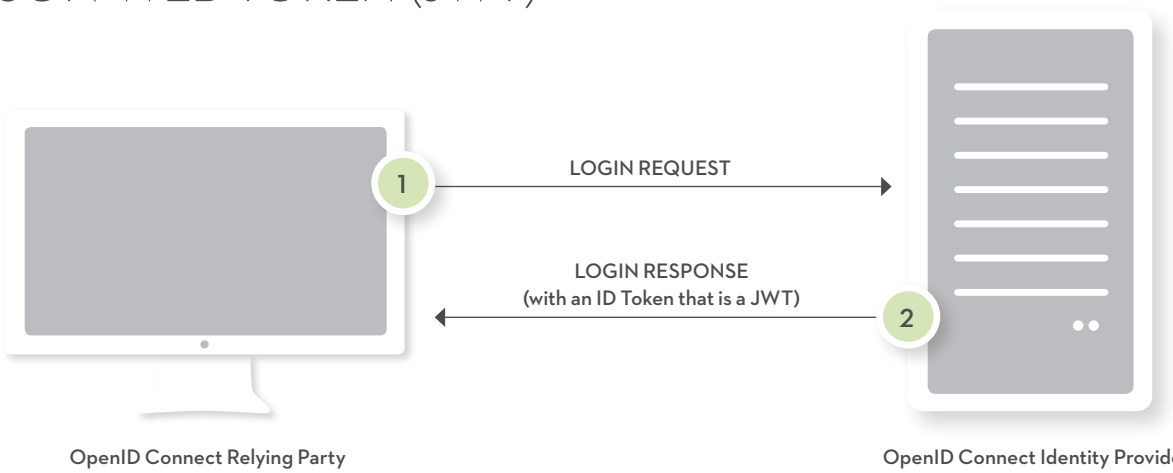
This specification was developed collaboratively based upon inputs from a number of independently developed precursor JSON token, signing, and encryption specifications. Over a dozen independent and interoperable implementations of the JWS specification are known to exist at this point, many of them in production use. The IETF JSON Object Signing and Encryption (JOSE) working group[17] has requested publication of JWS as an RFC—an IETF standard.

JSON Web Encryption (JWE)

JSON Web Encryption (JWE) is a means of representing encrypted content using JSON data structures. This specification complements the signature capabilities described in the closely related JSON Web Signature (JWS) specification. Encryption enables participants to pass confidential messages between themselves.

Several independent and interoperable implementations of the JWE specification are known to exist at this point, many of them in production use. Like JWS, publication of JWE has been requested as an RFC.

JSON WEB TOKEN (JWT)



JSON Web Key (JWK)

A JSON Web Key (JWK)[18] is a JSON data structure that represents a set of cryptographic keys. The JWK format is used to represent bare keys; representing certificate chains is an explicit non-goal of this specification. For instance, sets of JWKs are used by OpenID Connect to publish public keys and enable key rotation. In this use case, the signature on a JWT issued by the identity provider about the user having logged in is verified using keys published by the identity provider as JWKs.

Like the other specifications in this family, over a dozen independent and interoperable implementations of the JWK specification are known to exist at this point, many of them in production use. Like JWS, publication of JWK has been requested as an RFC.

JSON Web Algorithms (JWA)

The JSON Web Algorithms (JWA)[19] specification defines algorithms for use by JWS, JWE, and JWK (and therefore also algorithms used by JWT). Like the other specifications in this family, publication of JWA has been requested as an RFC.

WebFinger

WebFinger[20] defines an HTTPS GET based mechanism to discover the location of a given type of service for a given principal starting only with a domain name. These identifiers are URNs, which could be e-mail addresses, account identifiers, URLs, or other identifiers. For instance, OpenID Connect uses WebFinger to look up the identity provider for a user, given an identifier for the user such as an e-mail address.

OAuth 2.0 Specifications

The OAuth 2.0 family of specifications enables scoped authorization of third-party applications to HTTP-based services to occur without releasing end-user credentials to those applications. This scoped authorization process enables client applications to gain limited access to online resources with permission of the resource owner. See the photo sharing example in the next section for an example. The OAuth specifications use JSON data structures to represent structured data.

The OAuth 2.0 Authorization Framework

The OAuth 2.0 Authorization Framework[21] enables third-party applications to be granted limited access to an HTTP service on behalf of an end user by orchestrating an approval interaction between the end user and the HTTP service. This means, for instance, that I don't have to give an application my password on my photo site for it to be able to access my photos there for me and I don't have to give it the ability to change my photos just to read them. This specification is widely deployed on the Web and mobile devices today. Whenever you install an application on your phone and give it permission to access resources on your behalf, you're actually using OAuth. Likewise, both OpenID Connect and Facebook Connect[22] are built using OAuth 2.0.

> A rich suite of complementary and interoperable digital identity standards using JSON data structures and RESTful communication patterns has emerged and is in increasingly widespread use. These protocols retain much of the semantic richness of previous standards, while being easier to use across a broad range of Web development tools and platforms.

The OAuth 2.0 Authorization Framework: Bearer Token Usage

OAuth 2.0 Authorization Framework: Bearer Token Usage[23] enables clients to access protected resources by obtaining an access token, rather than using the resource owner's credentials. Access tokens are issued to clients by an authorization server with the approval of the resource owner. The client uses the access token to access the protected resources hosted by the resource server. This specification describes how to make protected resource requests when the OAuth 2.0 access token is a bearer token. A bearer token is usable by any party in possession of it.

JWT Profile for OAuth 2.0 Client Authentication and Authorization Grants

JSON Web Token (JWT) Profile for OAuth 2.0 Client Authentication and Authorization Grants[24] defines the use of a JWT bearer token as a means of requesting an OAuth 2.0 access token. It also defines how to use a JWT to authenticate an OAuth 2.0 client. For instance, this specification is used by OpenID Connect.

CONTINUED »

OpenID Connect Specifications

The OpenID Connect specifications enable Facebook Connect-like functionality from an open set of identity providers while also addressing some of the limitations of the OpenID 2.0 specifications. Put another way, it enables you to log into a relying party using a digital identity at an identity provider of your choice. These specifications build upon OAuth 2.0, JWT, JWS, JWE, JWK, JWA, and WebFinger. An explicit design point for the OpenID Connect protocols is enabling agents working on users' behalf, including browsers and mobile applications, to mediate users' identity interactions.

The OpenID Connect specifications were completed in February 2014. They are in production use by many organizations, including Google, Microsoft, Yahoo! Japan, Deutsche Telekom, Ping Identity, and Salesforce. For instance, when you're signing into Google+ or using Azure Active Directory, you're actually using OpenID Connect.

CONCLUSIONS

A rich suite of complementary and interoperable digital identity standards using JSON data structures and RESTful communication patterns has emerged and is in increasingly widespread use. These protocols retain much of the semantic richness of previous standards, while being easier to use across a broad range of Web development tools and platforms.

These protocols are being designed with an explicit awareness of the capabilities of modern browsers and Web development tools, including JSON support. Indeed, the designers believe that the already widespread adoption of these JSON-based digital identity standards demonstrates their usefulness for providing practical interoperable digital identity solutions. | SP | doi: 10.3789/isqv26no3.2014.05

MICHAEL B. JONES (mbj@microsoft.com) is an Identity Standards Architect at Microsoft and the author of the blog *Self-Issued: Musings on Digital Identity* (http://self-issued.info/).

REFERENCES

1. **Neuman, B. Clifford, and Theodore Ts'o. "Kerberos: An Authentication Service for Computer Networks."** ***IEEE Communications Magazine*****, September 1994, 32 (9): 33–38.** http://dx.doi.org/10.1109/35.312841
2. ***Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile.*** **RFC 5280. Internet Engineering Task Force, March 2, 2013.** http://www.rfc-editor.org/rfc/rfc5280.txt
3. ***Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0.*** **OASIS Standard, March 15, 2005.** http://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf
4. ***Web Services Security: SOAP Message Security 1.0 (WS-Security 2004).*** **OASIS Standard 200401, March 2004.** http://docs.oasis open.org/wss/2004/01/oasis 200401-wss-soap-message-security-1.0.pdf
5. ***WS-Trust 1.4.*** **OASIS Standard, February 2009.** http://docs.oasis-open.org/ws-sx/ws-trust/v1.4/os/ws-trust-1.4-spec-os.html
6. ***WS-SecurityPolicy 1.3.*** **OASIS Standard, February 2009.** http://docs.oasis-open.org/ws-sx/ws-securitypolicy/v1.3/os/ws-securitypolicy-1.3-spec-os.html
7. ***OpenID Authentication 2.0.*** **OpenID Final Specification, December 5, 2007.** http://openid.net/specs/openid-authentication-2_0.html
8. ***Information technology – ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER).*** **ITU-T X.690. International Telecommunication Union, July 2002.** http://www.itu.int/ITU-T/studygroups/com17/languages/X.690-0207.pdf
9. ***Extensible Markup Language (XML) 1.0 (Fifth Edition).*** **W3C Recommendation, November 26, 2008.** http://www.w3.org/TR/2008/REC-xml-20081126/
10. ***The JavaScript Object Notation (JSON) Data Interchange Format.*** **IETF RFC 7159, March 2014.** http://www.rfc-editor.org/rfc/rfc7159.txt
11. **Fielding, Roy Thomas. "Representational State Transfer (REST)." In:** ***Architectural Styles and the Design of Network-based Software Architectures*****, Chapter 5. Ph.D. Dissertation. University of California, Irvine, 2000.** http://www.ics.uci.edu/~fielding/pubs/dissertation/rest_arch_style.htm
12. ***JSON Web Token (JWT).*** **IETF Internet-Draft, October 24, 2014.** http://www.ietf.org/id/draft-ietf-oauth-json-web-token-30.txt
13. ***JSON Web Signature (JWS).*** **IETF Internet-Draft, October 24, 2014.** http://www.ietf.org/id/draft-ietf-jose-json-web-signature-36.txt
14. ***JSON Web Encryption (JWE).*** **IETF Internet-Draft, October 24, 2014.** http://www.ietf.org/id/draft-ietf-jose-json-web-encryption-36.txt
15. ***OpenID Connect Core 1.0.*** **OpenID Final Specification, February 25, 2014.** http://openid.net/specs/openid-connect-core-1_0.html
16. **Web Authorization Protocol (oauth) Working Group [webpage].** http://datatracker.ietf.org/wg/oauth/charter/
17. **Javascript Object Signing and Encryption (jose) Working Group [webpage].** https://datatracker.ietf.org/wg/jose/charter/
18. ***JSON Web Key (JWK).*** **IETF Internet-Draft, October 24, 2014.** http://www.ietf.org/id/draft-ietf-jose-json-web-key-36.txt
19. ***JSON Web Algorithms (JWA).*** **IETF Internet-Draft, October 24, 2014.** http://www.ietf.org/id/draft-ietf-jose-json-web-algorithms-36.txt
20. ***WebFinger.*** **IETF RFC 7033, September 2013.** http://www.rfc-editor.org/rfc/rfc7033.txt
21. ***The OAuth 2.0 Authorization Framework.*** **IETF RFC 6749, October 2012.** http://www.rfc-editor.org/rfc/rfc6749.txt
22. **Morin, Dave.** ***Announcing Facebook Connect.*** **Facebook Developers Blog, May 9, 2008.** https://developers.facebook.com/blog/post/2008/05/09/announcing-facebook-connect/
23. ***The OAuth 2.0 Authorization Framework: Bearer Token Usage.*** **IETF RFC 6750, October 2012.** http://www.rfc-editor.org/rfc/rfc6750.txt
24. ***JSON Web Token (JWT) Profile for OAuth 2.0 Client Authentication and Authorization Grants.*** **IETF Internet-Draft, October 21, 2014.** http://www.ietf.org/id/draft-ietf-oauth-jwt-bearer-11.txt

[NISO REPORTS]

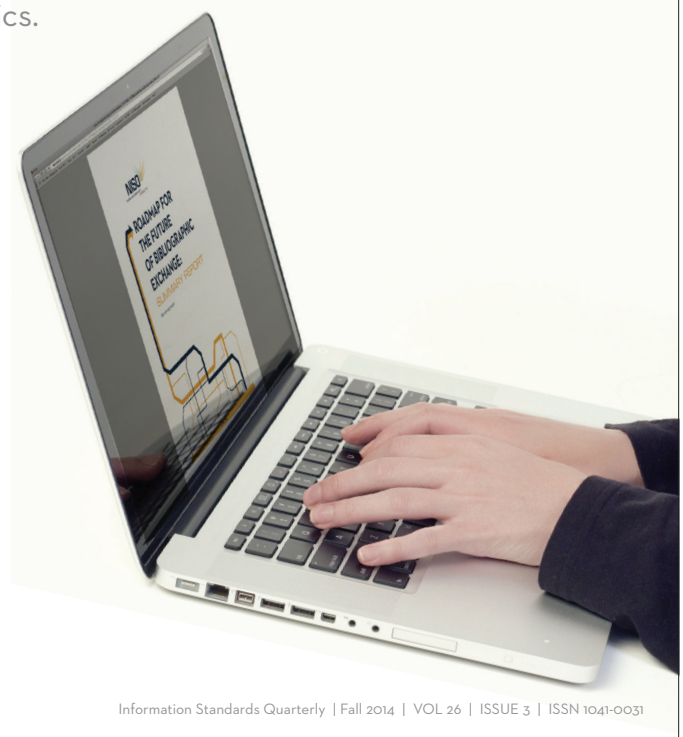
Nettie Lagace

NETTIE LAGACE

Pre-Standards Initiatives: Bibliographic Roadmap and Altmetrics

In areas where the need for standards is known but the specific areas and requirements are ill-defined, NISO often undertakes pre-standards work to identify and prioritize the standards or recommended practices that should be developed. In the past year and a half, NISO has undertaken two such initiatives. The first, started in December 2012 with a grant from The Andrew W. Mellon Foundation, was the **Bibliographic Roadmap Project** to develop a community roadmap for extending the usability of the new bibliographic framework into the global networked information environment. The second, begun in June 2013 with funding from the Alfred P. Sloan Foundation, was the Alternative Assessment **Metrics (Altmetrics) Initiative** to explore, identify, and advance standards and/or best practices related to a new suite of potential metrics.

Both of these projects completed their initial phase of community input and assessment and produced reports with recommendations of further actions NISO should take. This article summarizes the work of these initiatives and the recommendations.



Bibliographic Roadmap

In the current landscape of bibliographic exchange, most libraries are still creating and managing their extensive bibliographic data in MARC format. MARC, the lingua franca in libraries for over forty years, is often described as an outdated format, but its biggest liability in the modern web world is that it is unknown and unused outside of libraries. This uniqueness thus dooms library materials described with it to a siloed existence available within only

CONTINUED »

Given the diverse community that is impacted by bibliographic exchange as well as the tremendous investments made in existing MARC-based library systems and records, NISO proposed developing a roadmap for the high-level coordination of activities.

library-oriented systems. The vast majority of library users today, who no longer consider libraries as the first point of entry for most of their information needs, prefer accessing information via the larger networked world, which demands approaches to data that can be more easily shared, indexed, and linked.

Recognizing the need to advance bibliographic exchange, the Library of Congress (LC) initiated a community discussion on the Future of Bibliographic Control in 2006 and the report of its recommendations was published in January 2008. Since that report was issued, libraries have begun to embrace the concept of the Semantic Web and linked data and have implemented specific projects that are elements of a new paradigm for bibliographic exchange. Resource Description and Access (RDA), a structure developed by the Joint Steering Committee that is meant to replace the *Anglo-American Cataloguing Rules*, 2nd edition revised (AACR2), was published in June 2010 to provide a model for mapping some of MARC data into web resources, but the processes, workflows, and systems to support a full conversion to RDA are not yet in place. The Library of Congress in an announcement in October 2011 stated that the MARC standard as a carrier of bibliographic records is not sufficient in the web-based world.

Given the diverse community that is impacted by bibliographic exchange as well as the tremendous investments made in existing MARC-based library systems and records, NISO proposed developing a roadmap for the high-level coordination of activities to help avoid duplication and fragmentation of the bibliographic exchange community.

The work began with a two-day meeting in Baltimore in April 2013 attended in person and virtually by over 100 experts and participants, including librarians, system vendors, publishers, and consultants and vendors providing services around these. Eight major general areas to address were identified in that meeting:

- Business models
- Goals
- Interoperability
- Openness and sharing
- Prototyping
- Provenance/Authority
- Rules
- Users

Each of these themes was discussed in greater depth and over 40 ideas for potential actions to address them were collected and posted in the NISO Ideascale idea-sharing website. The Ideascale tool was discussed in a follow-up webinar and publicized to the community to encourage feedback on prioritizing the ideas. The two most highly-ranked ideas from Ideascale were taken forward to an open discussion session held at ALA Midwinter, January 2014, where specific projects that NISO could undertake were proposed. The two ideas and the proposed projects are:

Work to make vocabularies work across systems

- Work specifically to bring related vocabulary efforts together to take better advantage of expertise, tools, and existing best practices.
- Explore existing stores of vocabulary information (the Linked Open Vocabularies project is a good start) to identify problems, gaps, and potential for collaboration.
- Ensure that NISO's own published vocabularies are in a machine-accessible form and take advantage of advancing knowledge in vocabulary expression and management.

Improve the ability of our data to be consumed and manipulated

- Create a recommended practice or an informational document around the use of linked data and associated rights and their implications.
- Create a community recommended practice specifically for data contribution for corporate entities to utilize as a justification for their contributions and potentially to use as a shield, or partial shield, in regard to liability questions.
- Organize, evangelize, and manage an authority file as an additional/alternative Registration Agency for ISNI to expose the ISNI to communities not familiar with the standard.

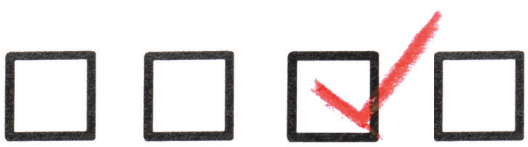
The activities that were determined, through community discussion to be part of the NISO Bibliographic Roadmap in large part aim to be applied to existing efforts and maximize

their usability as much as possible. It was recognized in many discussions that though the larger library community overall may seem to be hesitant in moving forward amid a fair amount of uncertainty in the lack of a solid technical framework, there is already much experimentation and many projects under way in diverse spaces. Further practical exploration of existing vocabularies, linked data tools, and methods for data contribution can help to reassure the community that the transition forward will not be endless and the value of what libraries already do will be enhanced.

NISO's leadership, via the Content and Collections Management Topic Committee is examining these prioritized Roadmap work items—as well as the other ideas generated throughout this process—for future action during 2015.

Altmetrics

Since Eugene Garfield's pioneering work in the 1960s, much of the research assessment work has been based upon citations. As a metric, citation reference counts have been an exceptionally rich source of accessible data upon which to draw conclusions about the quality of scholarship and will remain an important component of research assessment. The JIF (Journal Impact Factor), which measures journals' average citations per article, is one of the most used assessment measures, but such citation-based metrics are not keeping pace with the expanded scope of forms and usage that are presently available. Online reader behavior, network interactions with content, social media references, and online content management—all important indicators of scholars' interaction with research outputs—are not reflected in today's measures. Newer forms of scholarly outputs, such as datasets posted in repositories, software tools shared in GitHub, and algorithms or molecular structures are now commonplace but they are not easily—or if at all—assessed by traditional citation metrics.



The goal was to identify specific action items that NISO could pursue, particularly for the development of standards or recommended practices, to advance the use of altmetrics in the community.

These are among the many concerns the growing movement around alternative metrics, sometimes called altmetrics, is trying to address. In developing and applying new forms of altmetrics, many issues come up, such as:

- What exactly gets measured?
- How do we decide what the criteria are for assessing the quality of the measures?
- At what granularity should these metrics be compiled and analyzed?
- How long a period should altmetrics cover?
- What is the role of social media in altmetrics?
- What is the technical infrastructure necessary to exchange these data?
- Which metrics will prove most valuable and how do we decide?
- What types of assessment criteria could and should be applied to these new metrics to best assess the value of the analysis?
- How do we ensure consistent quality across providers?

In the first phase of NISO's Altmetrics Initiative, input from relevant stakeholders about these and other issues surrounding altmetrics was obtained through three in-person meetings and 30 in-person interviews. Recordings, documents, and other output from these meetings are archived on the Altmetrics Initiative webpage. The goal was to identify specific action items that NISO could pursue, particularly for the development of standards or recommended practices, to advance the use of altmetrics in the community.

The input received was summarized in a white paper, which identified a total of 25 action items in nine categories.

Definitions

- Develop specific definitions for alternative assessment metrics.
- Agree on proper usage of the term "Altmetrics," or on using a different term.
- Define subcategories for alternative assessment metrics, as needed.

Research Outputs

- Identify research output types that are applicable to the use of metrics.
- Define relationships between different research outputs and develop metrics for this aggregated model.
- Define appropriate metrics and calculation methodologies for specific output types, such as software, datasets, or performances.

CONTINUED »

Discovery

» Agree on main use cases for alternative assessment metrics and develop a needs-assessment based on those use cases.

Research Evaluation

» Develop statement about role of alternative assessment metrics in research evaluation.

» Identify specific scenarios for the use of altmetrics in research evaluation (e.g., research data, social impact) and what gaps exist in data collection around these scenarios.

Data Quality and Gaming

» Promote and facilitate use of persistent identifiers.

» Research issues surrounding the reproducibility of metrics across providers.

» Develop strategies to improve data quality through normalization of source data across providers.

» Explore creation of standardized APIs or download or exchange formats to facilitate data gathering.

» Develop strategies to increase trust (e.g., openly available data, audits, or a clearinghouse).

» Study potential strategies for defining and identifying systematic gaming of new metrics.

Grouping and Aggregation

» Identify best practices for grouping and aggregating multiple data sources.

» Identify best practices for grouping and aggregation by journal, author, institution, and funder.

» Define and promote the use of contributorship roles.

Context

» Establish a context and normalization strategy over time, by discipline, country, etc.

Stakeholders' Perspectives

» Describe main use cases for the different stakeholder groups.

» Identify best practices for identifying contributor categories (e.g., scholars vs. general public).

Adoption

» Identify organizations to include in further discussions.

» Identify existing standards to include in further discussions.

» Prioritize further activities.

» Clarify researcher strategy (e.g., driven by researcher uptake vs. mandates by funders and institutions).

Due to the number of potential action items, a follow-up survey was conducted to obtain further feedback on prioritizing the proposed actions. The top three "very important" items were:

» Promote and facilitate use of persistent identifiers in scholarly communications. (59.5%)

» Develop specific definitions for alternative assessment metrics. (54.3%)

» Develop strategies to improve data quality through normalization of source data across providers. (41.7%)

The NISO Business Information Topic Committee with input from the Altmetrics Steering Committee is evaluating the white paper, the comments received on it, and the prioritization survey and will be recommending one or more Working Groups for start-up by year-end 2014.

| NR | doi: 10.3789/isqv26no3.2014.06

RELEVANT LINKS

BIBLIOGRAPHIC ROADMAP

Bibliographic Roadmap Project webpage
http://www.niso.org/topics/tl/BibliographicRoadmap/

Project proposal
http://www.niso.org/apps/group_public/document.php?document_id=9975&wg_abbrev=ccm

Report with recommendations
http://www.niso.org/apps/group_public/download.php/13327/NISO_14007BibliographicRoadmapDevelopmentDoc_FINAL4.pdf

ALTMETRICS

Altmetrics Project webpage
http://www.niso.org/topics/tl/altmetrics_initiative/

Project proposal
http://www.niso.org/apps/group_public/download.php/11012/niso-altmetrics-proposal_public_version.pdf

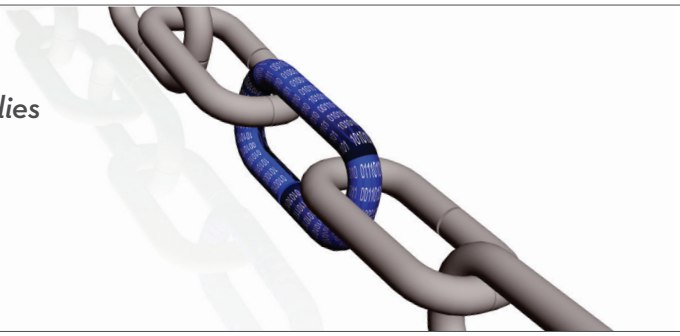
White Paper with recommendations
http://www.niso.org/apps/group_public/download.php/13809/Altmetrics_project_phase1_white_paper.pdf

Special Altmetrics issue of Information Standards Quarterly
http://www.niso.org/publications/isq/2013/v25no2

NW [NOTEWORTHY]

Linked Content Coalition Sets Ten Targets for a Digital Future

The Linked Content Coalition (LCC), a not-for-profit global consortium of standards bodies and registries, was formed to facilitate and expand the legitimate use of content in the digital network through the effective use of interoperable identifiers and metadata.



In its recent manifesto, the LCC has set out ten targets that it believes will best ensure that the digital rights data network operates as effectively as possible. The ten targets are designed "to ensure that every creator and every creation can be automatically identified on the net if they wish to be; that every creation can have machine-readable rights information linked to it (whether for commercial or free use); and that existing standards of different media types can be interoperable." The targets are:

1. **A global Party ID "hub"** – Rightsholders and "asserters" should be identified with an identifier linked to the ISNI "hub".
2. **Creation IDs for all** – Creations of all types should be identified to any required level of granularity.
3. **Right IDs** – Content rights should be identified distinct from, but linked to, the Creations to which they relate.
4. **Resolvable IDs** – Identifiers should have a URI form so they may be persistently and predictably resolved to multiple services within the internet.
5. **Linked IDs** – "Cross-standard" links between identifiers should use interoperable terms and be authorised by interested Parties at both ends of the link.
6. **Interoperable metadata** – Standard content and rights metadata schemas and vocabularies should have authorised, public mappings which enable terms and data to be automatically transformed from one standard into another.
7. **Provenance of Rights data** – The provenance ("asserter") of Rights declarations should be made explicit.
8. **Digital Rightsholder Statement ("DRS")** – Anyone should be able to make standardised, machine-interpretable public statements about rightsholdings in Creations.
9. **Conflict management** – Conflicts between public Rights declarations should be automatically identifiable so that their resolution can be managed.
10. **Linked fingerprints** – Where digital "fingerprints" or embedded "watermarks" exist, they should be mapped to registered Creation identifiers.

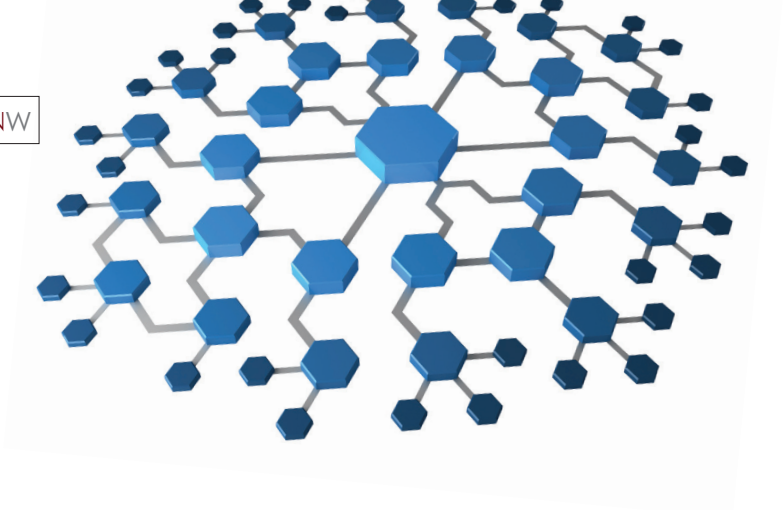
The LCC had previously issued their Framework, which includes the Rights Reference Model, Principles of Identification, and Principles of Messaging. The Framework "offers an integrated strategy which can be applied both "top down" and "bottom up", making use of existing schemas and infrastructure but describing ways of creating, aggregating and transforming complex, multimedia data to fill gaps in the network."

The six founder Board members of the LCC are EDItEUR, the International DOI Foundation (IDF), the International Press Telecommunications Council (IPTC), Movielabs, the National Information Standards Organization (NISO), and the PLUS Coalition. ■

Linked Content Coalition:
http://www.linkedcontentcoalition.org

The Ten Targets:
http://www.linkedcontentcoalition.org/#!10-targets/c1wpl

LCC Framework:
http://www.linkedcontentcoalition.org/#!lccframe/



W3C Provides Best Practices for Linked Data

While writing the *Linked Data Platform Specification*, the World Wide Web Consortium (W3C) Linked Data Platform Working Group also prepared a best practices document "to help system implementers avoid common pitfalls, improve quality, and achieve greater interoperability with other Linked Data systems." The Linked Data Platform specification and a primer on it are still in draft stage.

Specific practices recommended in the Working Group Note *Linked Data Platform Best Practices and Guidelines* are:

- Predicate URIs should be HTTP URLs.
- Use and include the predicate rdf:type to represent the concept of type in LDPRs.
- Use relative URIs.
- Avoid dot-segments in URIs of POSTed content or use with caution.
- Represent container membership with hierarchical URIs.
- Include a trailing slash in container URIs.
- Use fragments as relative identifiers.
- Prefer standard datatypes.
- Re-use established linked data vocabularies instead of (re-)inventing duplicates.
- Use qvalues properly.
- Respond with primary URLs and use them for identity comparison.
- Represent relationships between resources.
- Minimize server-specific constraints.

More details about these recommendations are provided in the full Working Group Note. The Note also refers implementers to two sources for existing vocabularies: the *Linked Open Vocabularies* website and a wiki on *Common Vocabularies / Ontologies / Micromodels*. ■

Linked Data Platform Best Practices and Guidelines: http://www.w3.org/TR/ldp-bp/

Linked Data Platform Specification: http://www.w3.org/TR/ldp/

Linked Data Platform Primer: http://www.w3.org/TR/ldp-primer/

Linked Open Vocabularies (LOV): http://lov.okfn.org/dataset/lov/

Common Vocabularies / Ontologies / Micromodels: http://www.w3.org/wiki/TaskForces/CommunityProjects/LinkingOpenData/CommonVocabularies

BISG Issues Revised and Updated Guide to Identifiers

The Book Industry Study Group (BISG) has published a revised edition of the *Guide to Identifiers*, formerly known as the *Roadmap of Identifiers*, in two different formats—a new interactive version for online use and a downloadable PDF.

Assigning ISBNs is second nature for book publishers, but a host of other identifiers, such as the ISNI, DOI, and ISTC, have specialized applications increasingly relevant to the publishing industry. With the use of more complex digital content that incorporates other media, each with unique identifier standards, an understanding of the various identifiers across the spectrum of intellectual properties used throughout all sectors of the publishing industry—digital, physical, and abstract—is essential.

BISG's *Guide to Identifiers*, version 4.0 explains the purpose of each identifier, lists its registration agency, maps its relationship to the various other identifiers, and provides additional information about its commercial opportunities and user guidelines. A highly visual interactive online version enables users to click on any particular identifier for the detailed information. The downloadable PDF, *Guide to Identifiers: Explanation of Identifiers* is a comprehensive reference document in a directory format, organized by identifier.

This document was developed and revised by the BISG Identification Committee, chaired by Phil Madans, Hachette Book Group.

This document is complementary to BISG's *Roadmap of Organizational Relationships*, a graphic of the key organizations important to the book industry. ■

***Guide to Identifiers*, version 4.0 interactive format: https://www.bisg.org/guide-identifiers**

***Guide to Identifiers: Explanation of Identifiers* PDF format: https://www.bisg.org/publications/guide-identifiers-explanation-identifiers**

***Roadmap of Organizational Relationships*: https://www.bisg.org/docs/Roadmap_of_Organizations.pdf**

| NW | doi: 10.3789/isqv26no3.2014.07

SD [STANDARDS IN DEVELOPMENT: *September 30, 2014*]

Listed below are the NISO working groups that are currently developing new or revised standards, recommended practices, or reports. Refer to the NISO website (www.niso.org/workrooms/) and the *Newsline* quarterly supplements, *Working Group Connection* (www.niso.org/publications/newsline/), for updates on the working group activities.

Note: DSFTU stands for Draft Standard for Trial Use.

WORKING GROUP	STATUS
Access and License Indicators (formerly Open Access Metadata and Indicators) Co-chairs: Cameron Neylon, Ed Pentz, Greg Tananbaum	Recommended Practice (NISO RP-22-201x) being finalized for publication following the public comment period.
Journal Article TAG Suite Standing Committee Co-chairs: Jeff Beck, B. Tommie Usdin	Revision of the JATS standard (Z39.96-201x) in development.
Journal Article Versions (JAV) Addendum Chair: Michael Dellert	Revised Recommended Practice (NISO RP-9-201x) in development.
Open Discovery Initiative Co-chairs: Marshall Breeding, Jenny Walker	Recommended Practice *Open Discovery Initiative: Promoting Transparency in Discovery* (NISO RP-19-2014) published.
Protocol for Exchanging Serial Content Co-chairs: Leslie Johnston, Kimberly Tryka	Recommended Practice (NISO RP-23-201x) in development.
Standard Interchange Protocol (SIP) Co-chairs: John Bodfish, Ted Koppel	Standard (NISO Z39.100-201x) in development.
SUSHI Lite Co-chairs: Paul Needham, Oliver Pesch	*Technical Report (NISO TR-06-201x) in development.*
SUSHI Standing Committee Co-chairs: Marie Kennedy, Oliver Pesch	Revision of the SUSHI Protocol standard (Z39.93-201x) at ballot.
US Profile of ISO 3166 Country Codes Chair: TBD	Working group being formed to develop standard (Z39.101-201x).

| SD | doi: 10.3789/isqv26no3.2014.08

Navigate through ISSNs:
The ROAD Directory and the ISSN Register

ISSN is the international identifier for serials
and other continuing resources, both print and electronic.

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INTERNATIONAL CENTRE

ROAD DIRECTORY OF OPEN ACCESS SCHOLARLY RESOURCES

+ **The ISSN Register** contains more than 1.7 million records produced by bibliographic experts and updated daily (more than 200 new records per day).
+ **ISSN Register** is the most accurate reference tool to find your way in the complex world of serials: retrieve short-lived titles, discover relationships between titles, switch from print to online version, key to manage new subscriptions.

Specific services:

+ **ISSN Portal:** Your web access to the ISSN Register;
+ **OAI-PMH protocol:** The ISSN web service for automatic updates at regular basis;
+ **ISSN Premium:** Customized processing of your data;
+ **Z39.50 Access:** For copy cataloguing.

Available formats: MARC 21, MARC XML, UNIMARC

New

+ **ROAD**, the Directory of Open Access scholarly Resources, is a free service supported by UNESCO that covers different types of online scholarly resources: journals, conference proceedings, academic repositories, book series.

Major purposes:

+ It provides a single access point to various types of online scholarly resources published in OA;
+ It uses the ISSN as a key identifier to aggregate data about the quality and reputation of OA resources;
+ It gives an overview of the OA scholarly content worldwide.

Main features:

+ Faceted and Map searches;
+ Search by country, subject, indexing service, journal indicator and by ISSN;
+ ISSN-based records enriched by data provided by DOAJ, Scopus, Latindex Catalogo, PsycINFO®, SJR, SNIP, The Keepers;
+ ISSN records freely downloadable and reusable

For more information, contact us at: sales@issn.org - ISSN International Centre

Tel : +33 1 44 88 22 20 - Fax : +33 1 40 26 32 43 - http://www.issn.org - http://road.issn.org