3-29-2024

Demystifying Shibboleth: Adapting to Web Browser Privacy Changes

Simon Robins
University of Dayton, srobins1@udayton.edu

Ben Daigle
University of Dayton, bdaigle1@udayton.edu

Demystifying Shibboleth: Adapting to Web Browser Privacy Changes

Simon Robins, MLIS,
University of Dayton Libraries, Dayton, Ohio
srobins1@udayton.edu
https://orcid.org/0000-0002-3264-5968

Ben Daigle, MLIS,
University of Dayton Libraries, Dayton, Ohio
bdaigle1@udayton.edu
https://orcid.org/0000-0001-7882-9239

Demystifying Shibboleth: Adapting to Web Browser Privacy Changes

Abstract

University of Dayton Libraries added Shibboleth as an additional form of authentication for its licensed e-resources beginning in summer 2023. A major impetus for pursuing Shibboleth are the upcoming web browser changes that will obfuscate users' IP addresses, set to occur in later 2023 and 2024 and something which will likely disrupt on-campus IP range access via EZproxy. Implementation of Shibboleth for an initial round of fifty-five e-resource platforms was relatively quick as a result of the University of Dayton's participation in the InCommon Federation of U.S. higher education institutions, also known as an "authentication federation." Methods for achieving the implementation involved entering Shibboleth entities within vendors' admin portals or working with the vendor representatives via email. Contrary to our previous understanding of Shibboleth, this implementation did not require extensive work on our end with our central IT office and typically required us to provide only a handful of entities directly to the vendor (all of which are anonymous entities). This article aims to share our workflow and lessons learned in the hope that other InCommon member institutions can follow suit.

Introduction

The aim of this article is to provide a detailed overview of a successful implementation of Shibboleth as an additional authentication method for library e-resources. In summer 2023, the University of Dayton Libraries enabled Shibboleth for approximately thirty of our most popular e-journal and e-book packages. This was followed by the successful configuration for another 20 platforms in September through November (see Appendix A for full list). A major impetus for enabling Shibboleth was the looming changes being proposed by major web browsers to ensure IP address privacy and the impact this will likely have for on-campus authentication[1]. We started configuring Shibboleth towards mid-July 2023, and by mid-October 2023, we were successful with the first 45. All of these configurations were achieved in one of two ways: either within the vendor admin pages for these platforms, or by emailing a vendor representative and having them configure it for us. All of the configurations were achievable as a result of the University of Dayton being a member of the InCommon Federation of U.S. higher education institutions, also known as an "authentication federation." Further, InCommon itself is a member of eduGAIN, an international interfederation service that aggregates and distributes metadata on behalf of regional identity federations such as InCommon, enabling members to collaborate without having to establish individual trust relationships with each other. Implementing Shibboleth as part of an authentication federation streamlined the process significantly, and it avoided us having to complete the often complicated task of working with a central university IT office to jump through numerous hoops on the backend with the university's configuration of Shibboleth (completing tasks such as importing metadata into our Identity Provider or sending our Identity Provider's metadata URL or metadata XML file to the vendor). As a result, this article will *not* be relevant to institutions who do not belong to authentication federations like InCommon or OpenAthens, and we realize that this excludes

[1] Google Privacy Sandbox, https://privacysandbox.com

many university and college libraries at institutions where the central IT office does not have the staffing or the funding to establish and maintain this type of membership. For those that do belong to InCommon, we realize that Shibboleth configuration can vary greatly across different universities. Configuration might not play out in the exact same way described here, but it will likely involve the same steps we describe, only it could involve releasing different entities and attributes than the ones we used. Our central aim is to demonstrate how Shibboleth configuration at certain libraries can be a relatively straightforward and quick process, and we fully advocate for it as an additional means to make access more seamless for faculty, staff, and students. To our knowledge, the configurations described in this article are no different from the configurations provided by OpenAthens, apart from the cost of OpenAthens and the central admin provided by an OpenAthens subscription. Lastly, our goal is not to explain in great detail how Shibboleth, SAML, or even EZproxy work on the backend. Instead our aim is to pave the way for those wishing to implement Shibboleth without having a comprehensive technical understanding of Shibboleth as a prerequisite.

Context & Background

Configuring SAML 2.0 with O'Reilly Safari Learning Platform

Shibboleth first came to our attention with the implementation of SAML (Security Assertion Markup Language) 2.0 authentication for the O'Reilly Learning Platform (also known as Safari E-Books). O'Reilly does not offer IP-based authentication with EZproxy, and our previous authentication method was very cumbersome and confusing to our users[2]. The implementation of SAML 2.0 was delayed several times for this platform, largely because we opted for a direct SAML-based integration between our institution and O'Reilly in lieu of the federated method via InCommon. O'Reilly is a member of InCommon but due to a stated limitation of the InCommon approach with their mobile experience, we decided to pursue the direct SAML option (C. Ellis, personal communication, March 11, 2022). In all, configuration took several years and was an arduous process, involving lengthy email chains with vendor representatives, our central IT office, and library staff about the security implications of releasing certain patron metadata attributes. The process was ultimately successful, but in hindsight, our key takeaway is that the process of implementing a direct SAML integration with an e-resource vendor can be a time-consuming effort involving multiple campus stakeholders, meetings, and configuration steps. Our discovery of federated authentication configuration through InCommon presented an exciting opportunity to get ahead of the upcoming browser changes at a faster pace and potentially streamline our patrons' experiences with accessing our e-resources.

Shibboleth, EZproxy, and IP Address Privacy

At the same time we were configuring SAML for Safari, we were closely monitoring the proposed changes to major browsers which would negatively impact IP authentication by hiding the users' IP addresses from the publisher platforms and databases while users are on-campus. While this change has yet to fully play out and is still mostly hypothetical at this point, it is worth taking a moment to outline how the issue will likely impact libraries across the world beginning in late 2023. Within the library

[2] Users previously had to select a link labeled "institution not listed?", enter their university email address, and then follow email instructions. This process is fairly standard across all OhioLINK member institutions.

community , there is a tremendous amount of confusion about how this will affect libraries. For example, it seems true that the changes will not affect off-campus EZproxy authentication based on a presentation from OCLC (Hamparian, 2023), but within this same presentation and on their website's FAQ, OCLC also states "if EZproxy has functionality based on the browser IP address, such as not proxying on campus users, that may be affected" (OCLC, 2023). This last part seems to apply to any campus using the excludeIP within their EZproxy config file, and this would therefore mean that many institutions would be negatively impacted for their on-campus users. At the University of Dayton, we use the excludeIP function heavily to allow direct access without requiring a login to any of our e-resources across all of our on-campus IP ranges. UD's percentage of residential undergraduate students who live on campus all four years is among the highest of any university in the country, and all of this on-campus housing resides within our university's IP ranges. As a result, we see the IP range privacy changes having a huge impact on our users' experiences accessing e-resources on campus. It is true that if IP ranges are made anonymous, users could still gain access to our e-resources via EZproxy while on or off-campus, but this would require the user to always reach an e-book or a journal article via a link with their library's proxy prefix.[3] Any previous workflows for on-campus users who relied on accessing content via Google or email alerts (links almost always without the EZproxy prefix) would now hit a paywall. Another way to put all of this is: the experience of on-campus becomes the same as off-campus.

From what we've been told by EBSCO and other publishers, access will be affected in a negative way, gradually over time, once the IP changes to browsers go through (EBSCO, 2023). In July 2023, EBSCO specifically summarized the upcoming changes and how they are expected to impact access and authentication, and they clarified two important points. First, they noted how the changes will not be sudden but will instead occur gradually beginning in late 2023. Second, they offered advice on how to prepare for the changes. Their recommendation: "single Sign-On, such as Federated Access, has been identified as one way libraries can future proof their access against evolving – and sometimes unpredictable – technologies outside our community's control" (EBSCO, 2023). This ran contrary to OCLC's presentations and FAQs on EZproxy, where the implication seems to be that libraries using EZproxy do not need to make any changes. At the same time, we are aware of EBSCO's OpenAthens product and the beneficial implications these changes will likely have on libraries' rationale to adopt the authentication platform, whereas OCLC's EZproxy product does not stand to benefit from these changes.

Regardless of whether these IP range changes are implemented by web browsers, we decided in late July 2023 that it would be advantageous to configure Shibboleth for our patrons on additional platforms. In our view, this implementation was entirely a "win-win" proposition: it would provide an additional mode of access to offset the likely disruption to workflows for on-campus users who rely on IP range authentication, while at the same time Shibboleth would not replace or disrupt our existing EZproxy configuration. This last point–the fact that the two authentication modes to not negatively interact with each other–was crucial in our decision to move forward. Moreover, the login screen for EZproxy looks identical for the login screen for Shibboleth (both are UD's campus-wide login screen)

[3] At UD, this prefix is https://libproxy.udayton.edu/login?url= followed by the platform's url, so for ScienceDirect it is https://libproxy.udayton.edu/login?url=https://sciencedirect.com, for example.

How Shibboleth differs from EZproxy

Unlike EZproxy, Shibboleth does not rely on IP ranges. Shibboleth is open-source software that separates the responsibilities of a service provider (SP), such as a publisher that provides access to content and related services, and an identity provider (IdP), such as a university that manages information about its users and their various attributes including their role, affiliations, and personally identifiable information. This model frees the service provider from the tasks of managing and securing user credentials, and it helps the identity provider ensure that only the data that is necessary to facilitate appropriate access for appropriate users is released to the service provider. Additionally, once a user has signed into their identity management system, Shibboleth can help facilitate access to other service providers with which there is an established trust relationship without prompting for additional logins. Both the service provider and the identity provider exchange information using the Security Assertion Markup Language (SAML), an XML-based open standard designed to exchange identity-related information. For the end user, the key feature that Shibboleth enables is an "Access through your institution" button (or some variation on it) located in most publisher platforms, such as Wiley Online Library, IEEEXplore or ScienceDirect (**see figure 1)**. Even when connecting to a resource via EZproxy, this link appears for users when they are outside of ExcludeIP ranges, and it often appears even when users are authenticated on campus.

Figure 1. A typical example of a vendor placing the "Institutional Sign In" link front and center

For platforms that do not have Shibboleth enabled, off-campus users who do not select a proxied link (i.e. via Google) will reach a deadend when they select this "institutional sign in" option to access through their institution. This deadend can prove particularly confusing because the university/college name might not appear at all when the end user selects the option for institutional sign in, or their institution might appear under a dropdown list of institutions, but after selecting the link to login, the page will not allow for access and provide the end user with a message stating something along the lines of "your university does not provide access, please contact your library administrator." When this occurs in platforms to which the library has an active subscription (but without Shibboleth configuration), both

of these outcomes will likely create a false understanding of what the patron actually has access to through the library.[4] Figure 2 provides an example of what this looks like for the Mintel platform. The first screenshot shows how the University of Dayton appears as an option based on our participation in eduGAIN (something which appears automatically), while Figure 3 shows the error message after an attempted login through Shibboleth. The user was able to enter their campus-wide login credentials, but the authentication was unsuccessful because Shibboleth was not configured for the Mintel platform. At the same time, the university *does* subscribe to Mintel and provides access via EZproxy. An off-campus user at this point would need to know about the difference between these authentication methods, go to the library website and select the Mintel link with the proxy prefix. Unless they have been trained to do so, it is highly unlikely that they would intuit this option based on the red error message in Figure 3 from the failed authentication.

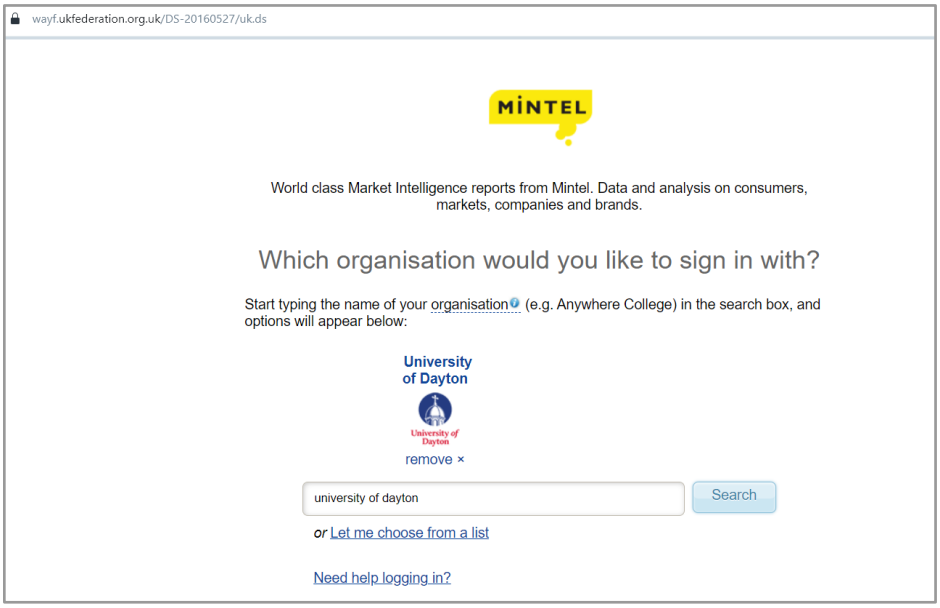


Figure 2. The University of Dayton appears as an option when searching on the "Which organisation would you like to sign in with?" page because Mintel and InCommon, of which the University of Dayton is a member, are both members of eduGAIN.

[4] Frustratingly, these "do not have access" messages will occur even when the institution does have a subscription to the resource because it is entirely out of sync with EZproxy.

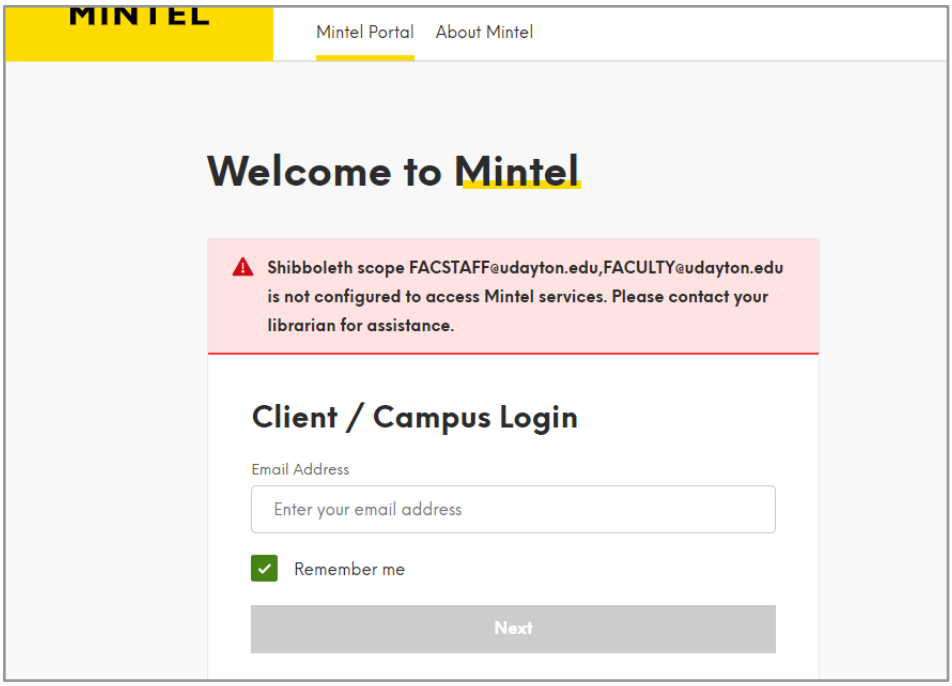


Figure 3. The end user sees this screen for the Mintel platform when they click the "institutional sign in" link from off campus. When they search for the "University of Dayton", they find their institution and logo (as seen in the top part of the image). This takes them to their campus-wide login (not pictured), yet after they authenticate, they see the error message pictured in the second part of the image.

Conversely, when Shibboleth is enabled, the user who selects the "Access Through Your Institution" link will find their university in the dropdown, be routed to their campus-wide login, and be able to authenticate to the library's configuration of that subscription. Crucially, this allows users to authenticate with publisher platforms while on or off campus without needing to visit the libraries' website to locate a proxied link from a list of databases or publisher websites. While the anticipated browser privacy changes will change the experience for on-campus users who may have grown accustomed to accessing e-resources without being prompted to login, the implementation of Shibboleth will result in a consistent user experience regardless of the user's physical location. Shibboleth, therefore, fills a gap created by these web browser changes by allowing on-campus users, who previously relied on automatic IP authentication, to stumble across their university within the list of "Access through your institution" options and be re-routed to their institution's single sign-on (SSO) page (as opposed to getting the impression that their library doesn't provide access at all).

As single sign-on software, Shibboleth also provides the added benefit of remembering a user's institutional affiliation across multiple platforms. For example, if the end user authenticates via Wiley Online Library using Shibboleth, and then comes across IEEEXplore (again, not via the library's website), the functionality of Shibboleth's cookies will auto-populate the user's institution when they click "Access through your institution" within IEEEXplore. The same would occur if they started in IEEExplore and went to Wiley Online Library. This process would occur for all users on and off campus. For all these reasons, we decided to explore Shibboleth for other platforms.

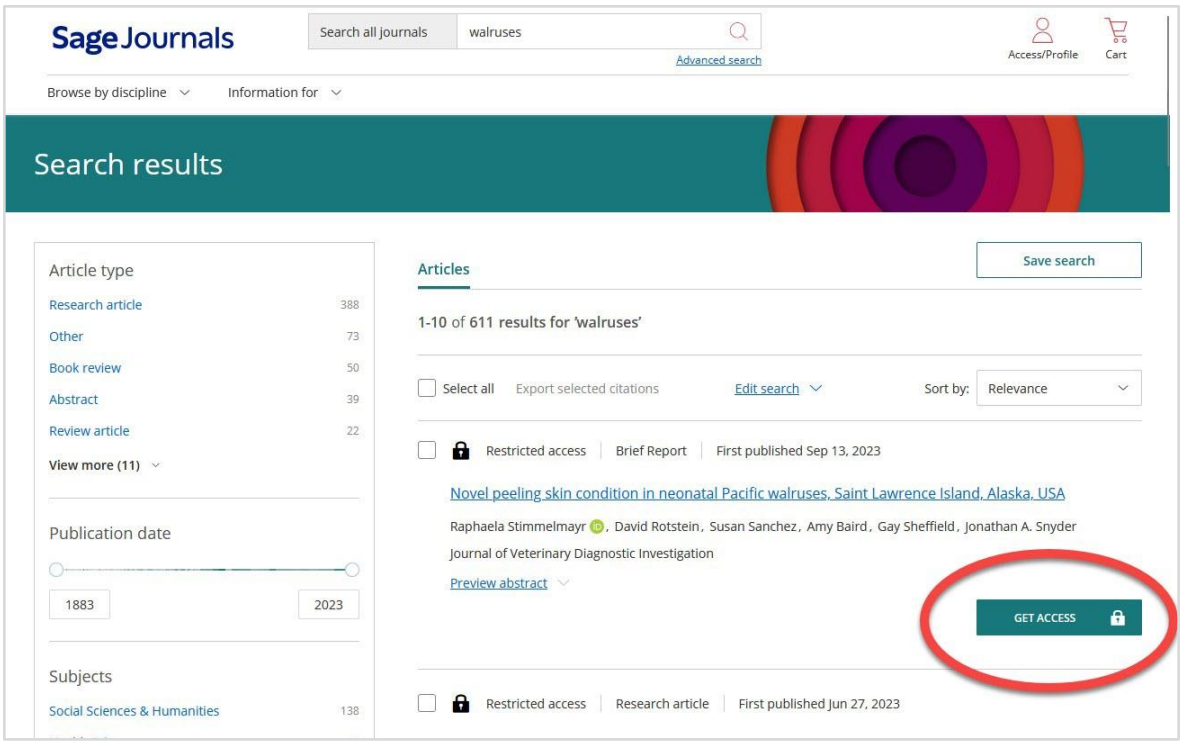


Figure 4a. Typical "Get Access" link provided to unauthenticated users within the Sage Journals platform.

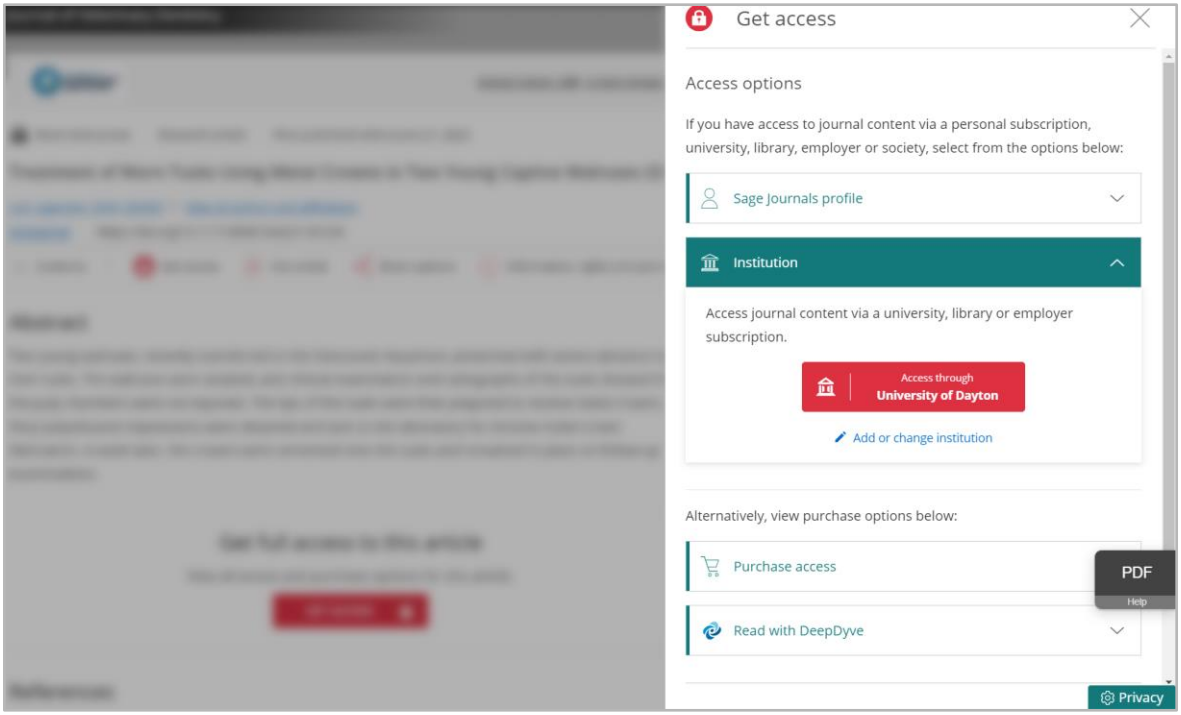


Figure 4b - Note the platform "remembering" the University of Dayton as a result of previous logins using Shibboleth (either within this platform or within other platforms such as Wiley Online Library or IEEExplore)

However, the proposed privacy changes to the major browsers are also likely to affect the single sign-on experience. In addition to IP masking, browser vendors are phasing out support for third-party cookies, which have been employed heavily by advertising and marketing firms to track users' browsing histories in order to deliver targeted ads based on previous browsing behavior. Unfortunately, this is the same technique used by federated authentication technologies to "remember" users' institutional affiliations as they visit different publisher websites, saving them the step of logging in repeatedly at each site. In November, 2023, SeamlessAccess, the organization working to develop the technology that "remembers" a user's institutional affiliation when searching across publisher platforms, posted an announcement about the effects of privacy changes in Google Chrome on the behavior of the "Access through your institution" button (SeamlessAccess, 2023, November 16). REFEDS (2023), a community of technologists, publishers, and practitioners representing the research and education sector, have been collaborating on solutions to the challenges to identity persistence caused by the deprecation of third-party cookies. Their recommendations will likely influence how federated authentication and SeamlessAccess will continue to function with Federated Credential Management (FedCM), the technology under development by the major browser vendors.

Literature Review

There is a significant amount of literature documenting the exploration and eventual decision not to adopt Shibboleth as a federated authentication option, and this especially applies to the state of Ohio. Much of this literature has to do with NISO's "Resource Access in the 21st Century" (RA21) initiative in 2018 and 2019. This initiative "provides recommendations for using federated identity as an access model and improving the federated authentication user experience" (NISO, p. 5). Shibboleth was listed as one of the options, and this initiative also clearly laid out what the end user experience should look like within the publisher platforms when it comes to identifying the users' institution (p. 19). As documented by several blog posts, columns, and articles at the time, North American librarians, unlike their European or United Kingdom counterparts, were broadly vocal in their opposition to RA21 (Hanson, 2018; Janicke Hinchliffe, 2018; Kraft, 2019; Pawlowski & Beadles, 2018; Schwing, 2018).

In late 2019, University of Minnesota librarian Nancy K. Herther summarized this outcry in an article for the magazine "Online Searcher," along with interviews conducted with 70 information professionals.[5] The article extensively details why numerous voices–especially in legal and medical libraries–were skeptical about whether publishers would adhere to what the standard called for and not track users who authenticate via federated platforms like Shibboleth (p. 38). It also contains a section with the response from RA21 creators at NISO, who offer their explanation for why concerns of security and privacy are unfounded. In hindsight, these refutations by NISO personnel seem to have done little to assuage librarians' concerns in the context of North American libraries, arguably because at the time very few libraries had implemented federated authentication. Herther summarizes what they see as the heart of the issue: RA21 details are "highly technical, far more so than those understood by information professionals," while also urging LIS professionals to participate in the discussion because "our voices are critical in the development of RA21 and future standards" (p. 40).

[5] Through these interviews, Herther found "many expressed serious concern based on the limited amount of information that has been presented" but still urged these same professionals (and the LIS professional community) to participate (p. 41).

Specific to Ohio and the OhioLINK consortium, in 2018 there were a handful of presentations delivered at a NISO event (Pawlowski & Beadles, 2018; Schwing, 2018). Theda Schwing analyzed what it would hypothetically involve for OhioLINK institutions to switch to federated authentication, noting numerous challenges preventing a successful switch: "funding will be complicated, the project needs to fit IT's existing goals, & there are many patron types that won't have network logins" (Schwing, 2018). Likewise, Pawlowski and Beadles, presented slides detailing the challenges OhioLINK libraries would face trying to implement federated authentication. Other presentations from the same day outlined how the cost would be significant to implement Shibboleth (Hanson, 2018).

Writing on behalf of an OhioLINK member library at Cleveland Clinic, Michelle Kraft wrote several blog posts and an article discussing the unique challenges facing medical libraries when it comes to clinicians who rely on IP authentication within highly securitized clinical networks (individuals who would almost certainly push back if they were told they would need to start authenticating to access peer-reviewed literature for clinical decision-making) (Kraft, 2018 & Kraft, 2019). In her 2019 article, she does outline the benefits of federated authentication, but leans more towards her primary concern that “user identity and privacy are significant concerns” (p. 77). Even the willingness of institutions’ central IT offices is a major concern for Kraft because the “primary focus (of an institutions’ central IT office) is control of an institution’s network, infrastructure, and security as a whole, not opening access to library resources” (p. 80).

In the lead up to the release of RA21, NISO weighed in again in 2019 when their Associate Director for Programs published a column promoting the advantages recommended practice could bring to the library community (Carpenter, T. A., 2019). He highlighted how “no additional information is required beyond that this user is affiliated with this institution, and for RA21, the recommendation is that the minimal amount of metadata for the service should be sent” (p. 194). He also highlighted how the adoption of RA21 would take several years, and “during this time, traditional authentication methods, such as IP-based authentication and proxy servers, will continue to be supported” (p. 194).

What seems especially surprising in hindsight is how these commentaries *might* be a major contributor to the current lack of adoption of Shibboleth in the United States. Meanwhile, as stated at the time in 2019, RA21 was made to fit the EU’s General Data Protection Regulation (GDPR) and might have made things more secure for those libraries who did adopt it (Herther, p. 40). One can speculate that the absence of a regulatory framework in North America similar to GDPR likely resulted in confusion about RA21, while in Europe RA21’s adherence to GDPR helped to allay any fears over privacy concerns.[6]

Despite these earlier criticisms, in more recent years there have been several leading voices calling for a move away from IP authentication, along with commentaries on what the future of library authentication might look like. In 2020, Thomas Dowling, Director of Technologies at Wake Forest University, wrote a column calling into question the library community’s continued usage of IP authentication. The author provides a fairly detailed overview of the prior twenty-five years of IP authentication–from the 1990s when most users authenticated from on-campus IP ranges, to the growth of off-campus users and the need for an intermediary proxy server, to our current situation where users often have a drastically different experience when off-campus than they do from on-

[6] As will be discussed later in this article, it does not seem to be the case that Shibboleth, as we’re implementing it at UD, releases any personal information for the end user to the vendor.

campus (pp.41-42) As he puts it rather bluntly, “any model that starts with ‘Don’t click the link to the content you want’ is fatally broken” (p. 42). Dowling concludes by calling for federated identity management and points to the past criticisms of security and privacy, noting how the information exchanged can be as minimal as “Yes, this is a valid user,” or “No, this is not a valid user” so long as the institution “explicitly limit[s] the information sent” to avoid “inadvertent data exposure” (p. 44)**.**[7] The author also discusses RA21. Dowling concludes by hypothesizing that “the 2020s will almost certainly see the first major change to library authentication since the 1990s” (p. 46)**.** In many ways this article on UD’s experience became a case study presenting what we hope was a successful implementation of what Dowling called for in his column.

In late summer 2022, Aaron Tay’s chapter "Improving Access to and Delivery of Academic Content from Libraries: A Roundup" similarly discussed what librarians should anticipate in the years ahead as SAML-based authentication methods become more prevalent. He presents three hypothetical long-term scenarios over the next ten years: 1) OA takes a more prominent role, and undercuts the need for authentication (the author thinks this is the least likely scenario); 2) a hybrid scenario where IP authentication is necessary for certain resources, while SAML-based authentication is available for others; or 3) wide-adoption of SAML-based authentication (p.46). While not exactly a consensus, this study and the one by Dowling do represent an emerging conversation on how authentication will likely change.

In terms of case studies on implementations of federated access solutions, there have been a number of recent publications on OpenAthens. Li, H., Holly, C., & Goodrich, T. (2022) discusses an implementation of OpenAthens at the University of Tennessee at Martin. Ruenz, M. M. (2022) at Wheaton College. After migrating to PrimoVE, the CARLI consortium trialed OpenAthens for three years (through June 2023) to potentially solve proxy issues. They also addressed the price: “The outright subscription cost for the self-hosted EZproxy configuration is significantly cheaper than the cost to offer authentication through OpenAthens” (p. 163). Despite this cost, there are far more institutions publishing about their experience switching from EZproxy to OpenAthens than there are institutions publishing on their experience migrating to any other federated authentication system.

As for recent publications focusing on the implementation of Shibboleth as part of an eduGAIN federation, we could only find one article. In 2021, librarians in Bangalore, India discussed a Shibboleth implementation at J.R.D Tata Memorial Library at the Indian Institute of Science (Jayakanth, F., Byrappa, A., & Visvanathan, R.). Their decision to implement Shibboleth was brought on by the surge in remote users during the COVID-19 pandemic (p.3). Through their implementation, they did note an increase in COUNTER 5 statistics, showing usage of “subscribed resources for the period of January 2020 to October 2020…increased by nearly 20 percent over the last year for the same period” (p.10). In general, their publication is an example of the type of case study on Shibboleth authentication across e-resources that this study aims to accomplish. We feel fairly confident that we are the first to publish on this type of

[7] Dowling also addresses the walk-in user dilemma: “Unfortunately, implementing an authentication system that removes IP access and requires all users to provide login credentials excludes one category of valid users. Many libraries explicitly serve walk-in users and license online content to include access for them. As walk-ins, physically present in the library, they are well served by IP authentication. This is a situation in which authentication by location works well, because the individual is not in the user database.”

implementation in a North American context; to date, there have either been publications on OpenAthens or implementations of Shibboleth outside of North America.

Representing the publisher and vendor perspective, Lloyd (2020), CEO of Liblynx and a member of SeamlessAccess, a service that emerged from the RA21 initiative with a set of tools and standard design elements for publishers to create a consistent user experience across content platforms, offers perhaps one of the clearest explanations of federated authentication in the literature. He disputes the reasoning posed by some in the library community that EZProxy and IP-based authentication are more effective at preserving privacy. He points out that IP addresses can be used to identify individuals and that users who avail themselves of a publisher platform's personalization features often need to share individual credentials. He also notes that when the need to block access from compromised accounts arises, it is a "blunt tool" since it is based on IP address and can sometimes mean blocking an entire institution's access if that IP address is the one associated with EZproxy. Regarding concerns over the release of attributes associated with an individual patron, such as name, email, or status, Lloyd clarifies that the individual's identity provider (IdP) controls the release of this metadata and cannot be extracted by the service provider (SP).

Zhu (2023), representing the Institute for Electrical and Electronics Engineers (IEEE), reports on an increase in full-text usage on the IEEE platform from users of federated authentication options like Shibboleth. "Users coming from federated authentication stayed on the platform longer, visited more often, viewed more pages, and had higher full-text usage." (Zhu, p. 312). Zhu also describes how during the pandemic, some publishers recognized an opportunity to simplify the authentication experience for library users. At IEEE, the publisher developed a pilot project in which they proactively downloaded metadata from eduGAIN for subscribing libraries in Canada and populated their platform's institutional login menus, reducing IEEE's reliance on libraries to configure their federated authentication options. However, depending on the individual libraries' implementations of federated authentication at their home institutions, patrons from those institutions had mixed experiences.

Methods: Enabling Shibboleth at the University of Dayton

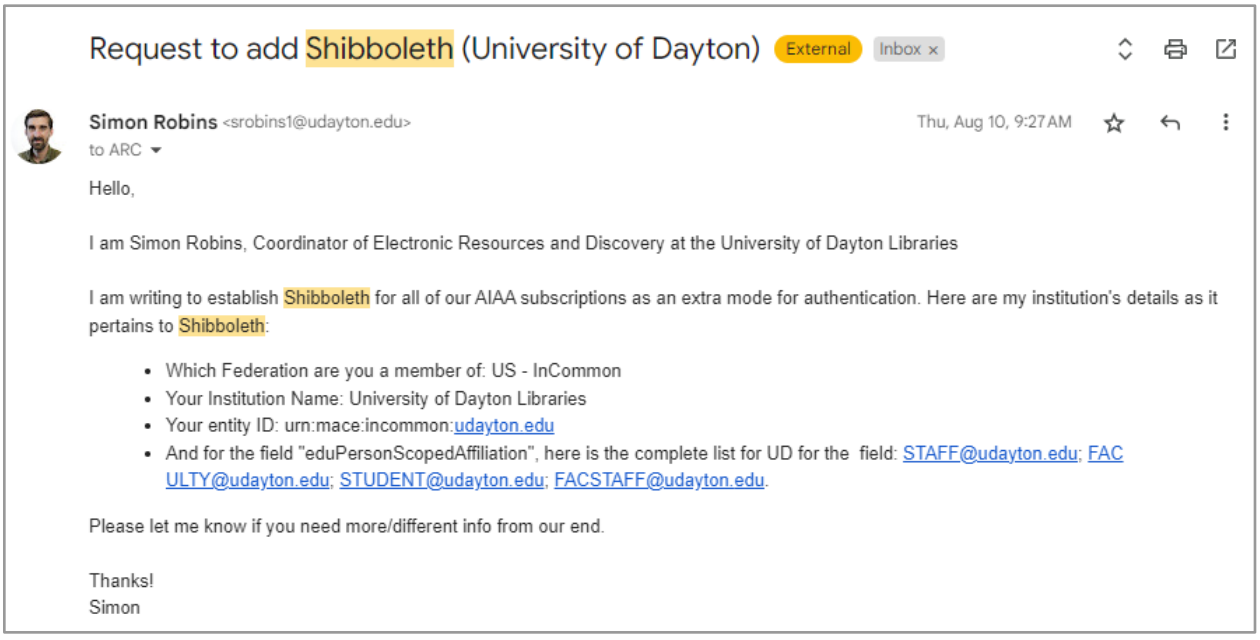
Initial test with Sage Journals

The first step in the process was to test turning on Shibboleth with one of our e-resource platforms. We noticed several of our prominent e-journal publisher platforms contained sections labeled “Shibboleth / OpenAthens,” providing fields to enter attributes, so we selected one of these, Sage Journals, as a test platform. The authors of this study worked together to assess what it would involve to turn on Shibboleth for more platforms. Based on our internal risk assessment of potential issues that could occur, we decided the benefits outweighed the drawbacks to working with a vendor to see what would occur once Shibboleth was turned on. The Sage admin portal specifically asked for our Shibboleth Entity ID and, optionally our Organization/unit ID. Using the information we had gathered from our central IT office when we configured Shibboleth for Safari, we went ahead and submitted the form with what turned out to be the wrong entityID, and we received an error message. Based on this, we simply emailed Sage’s support team to seek assistance. The Sage rep suggested using the entity ID publicly listed for the University of Dayton in eduGAIN (urn:mace:incommon:udayton.edu). This last part, we

quickly found out, is a key requirement to allow for a straightforward implementation of Shibboleth, as opposed to the more manual implementation with platforms like Safari. The Sage representative was very clear that they expect customers using Shibboleth to be registered with eduGAIN, and so far as we can tell, this was a prerequisite for adding Shibboleth to all the other platforms discussed in this study. Any institution interested in configuring library e-resources with Shibboleth can verify whether their institution participates in eduGAIN using their public databases at the following URL: https://technical.edugain.org/eccs. The process with Sage did require a few emails with the vendor, but mostly this had to do with us entering an incorrect entity for the "Organization/unit ID". It turned out that this field should remain blank for our institution, meaning that configuration for Sage only required entering one entity ID for our institution.

Additional Platforms

Based on the success with Sage, we proceeded to implement Shibboleth with as many platforms as possible, and we started with our most heavily used platforms (such as ScienceDirect, Wiley Online Library, Taylor & Francis Online, Oxford Academic, SpringerLINK, Cambridge Core, EBSCO, and JSTOR). Typically our implementation of Shibboleth went one of two ways. Either we were able to enter our entities within a vendor's admin portal and we would successfully test it within 24-48 hours, or we would have to email the vendor's support team and have them make the update for us. When the latter option was required, the implementation was typically more complicated, requiring some degree of troubleshooting. Figure xx is a screenshot of a sample email sent to a vendor. This same template was copy and pasted for reuse with many vendors.



Request to add Shibboleth (University of Dayton) External Inbox ×

Simon Robins <srobins1@udayton.edu> Thu, Aug 10, 9:27 AM
to ARC

Hello,

I am Simon Robins, Coordinator of Electronic Resources and Discovery at the University of Dayton Libraries

I am writing to establish Shibboleth for all of our AIAA subscriptions as an extra mode for authentication. Here are my institution's details as it pertains to Shibboleth:

- Which Federation are you a member of: US - InCommon
- Your Institution Name: University of Dayton Libraries
- Your entity ID: urn:mace:incommon:udayton.edu
- And for the field "eduPersonScopedAffiliation", here is the complete list for UD for the field: STAFF@udayton.edu; FACULTY@udayton.edu; STUDENT@udayton.edu; FACSTAFF@udayton.edu.

Please let me know if you need more/different info from our end.

Thanks!
Simon

Figure 5. Example of email sent to multiple publishers.

For the admin portals which allowed us to enable the feature, certain platforms use the same third party for their portals. This made the process fairly straightforward because it allowed us to enter the same entities in the exact same way and be fairly certain it would work. A key example of this was the "Silverchair" admin portal architecture. These portals required a few more entities, specifically, the

ScopedAffiliationID. In this case the entity was obtained from our central IT department, but to our knowledge is a fairly universal structure; for us it is FACULY@udayton.edu; STUDENTS@udayton.edu; STAFF@udayton.edu; FACSTAFF@udayton.edu. We were told by at least two vendors that the "FACSTAFF" entity was unnecessary, and it was removed.

For the third-party provider of vendors' admin interfaces "Atypon", we did experience some degree of difficulty, and at one point, we even experienced the exact same issue with ACM Digital Library, SPIE Digital Library, and Wiley Online Library (all three were producing the same error message after the vendors representatives attempted to implement Shibboleth). From our end, this required us to test logging in from an off-campus network (we use the Opera browser with a VPN configured to North America or Europe), and then respond to the respective vendor representatives to confirm whether or not it worked. In the case of ACM and Wiley, they asked us to authenticate to their platforms, enter URLs to show our identities (for example with ACM the urls are https://dl.acm.org/snoop and https://dl.acm.org/action/showIdentities), and then send the results as a PDF or as html download. Eventually SPIE determined the issue was occurring because our university has two eduPersonEntitlement values, and for some reason, these two entities were separated by a comma when they should have been separated by a semicolon. Once they switched the comma to a semicolon, access was restored: urn:mace:dir:entitlement:common-lib-terms; urn:mace:incommon:entitlement:common:1. Since the authentication error message was the exact same for Wiley Online Library and ACM Digital Library, we correctly suspected that this fix in SPIE would work as a solution for the other platforms, so we informed the reps for these companies about SPIE's solution, and it resolved the issue in both cases.

The second unique example was EBSCO. Unlike nearly all the other platforms discussed up until now, EBSCO's database and EDS discovery layer differ in that the individual results are discoverable via commercial search engines such as Google. This undermines the major need for Shibboleth because one can assume that the end user is required to know about the database names (Academic Search Complete, CINAHL, etc) and their entrypoint within the library's web presence *before* they access them. Despite this, we still investigated Shibboleth for EBSCO because we were aware of the possibility to configure Shibboleth which allows for the end user's personal account to be synced to their Shibboleth authentication. This syncing is not present with any of the other platforms we have configured with Shibboleth, but it is present with our configuration of SAML with Safari. This syncing allows for a more customized experience, most notably by retaining the user's search history and their custom folders with saved results.

At the time of writing, we still have not implemented this for EBSCO, but we have implemented Shibboleth as a form of authentication for all EBSCO databases and our discovery layer, and in the process, we have discovered an advantage to this configuration related to EBSCO's linking structure and its ability to provide authentication via cookies and via Shibboleth. Whereas in the past we have always prefixed our EBSCOhost database links with EZproxy, we now have a way to link to them without any prefix, instead using a url structure which includes "authtype=cookie,ip,shib". In full, an example using Shibboleth looks like this:

https://search.ebscohost.com/login.aspx?authtype=cookie,ip,shib,uid,user,url&custid=s9003728&groupid=main&profile=ehost&defaultdb=sih

This setting instructs EBSCO to attempt authentication in the order specified by the values in the authtype parameter. It first tries cookies, then IP address based on the address ranges we have on file with EBSCO, and finally Shibboleth. When users reach this Shibboleth option, it then adds a cookie, which in turn allows for returning off-campus users to authenticate without having to enter a username or password, even after their browsers have closed or their computers have been shut down[8]. We see this as a major benefit because previously off-campus users would have to always authenticate for EZproxy links, even if they had a cookie recorded by EBSCO.[9] Lastly, EBSCO has extensive documentation on how to enable Shibboleth within EBSCOadmin, and their support team was available to assist with the process. EBSCO did not require us to send emails with our Shibboleth attributes, and instead we were able to simply enable it within the "Authentication" tab in EBSCOadmin (as seen in Figure 6). To date, we have changed the links for roughly 36 EBSCO subject databases within our A-Z list to solely rely on this new url structure. This does not rely on EZproxy at all for initial access to the databases, but any link outs from these databases, or permalinks pulled from EBSCO still use EZproxy.

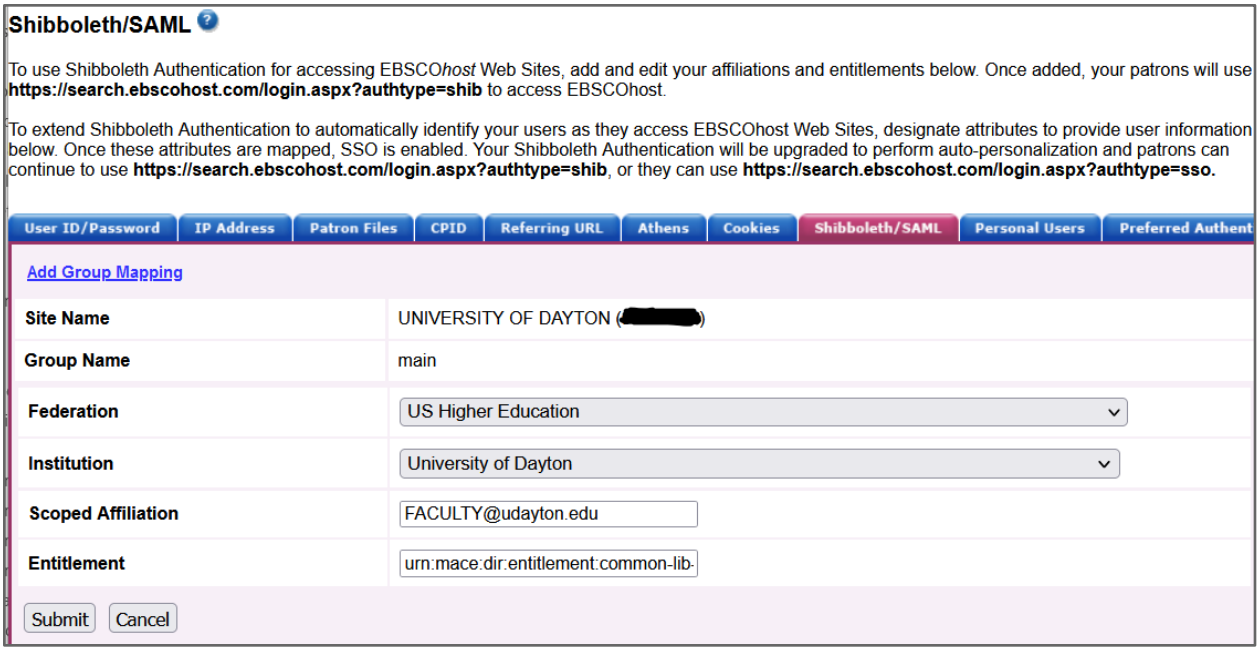


Figure 6. EBSCOadmin interface section for authentication, where under the "Shibboleth/SAML" tab, the federation and institution can be easily searched for. Each Scoped Affiliation is entered individually, pictured above is the entry for UD faculty.

Out of these configurations came an additional change to implement. Because the base URL of our OpenURL resolver typically did not include our EZproxy prefix, authenticating via Shibboleth caused these links to fail. Accordingly, we added our EZproxy prefix in all cases where we had registered an OpenURL with the vendor. This resolved the issue, and fortunately, when the end user logs in from off-campus via Shibboleth and clicks on an OpenURL link with our EZproxy prefix, they are not required to

[8] Of course, this only applies if the user has the more default setting where cookies are not deleted whenever they close their browser

[9] While the authors do anticipate that the upcoming browser changes will impact users' experiences navigating across publisher platforms because of their reliance on third-party cookies, they do not believe this will because it would likely be considered a "first-party cookie."

authenticate again, even though they are switching from Shibboleth in the vendor platform to EZproxy in the link resolver, specifically EBSCO's Full Text Finder. For EBSCO databases and EDS, the introduction of Shibboleth required us to change the "Preferred Authentication Order for Persistent Links" field to "cookie, ip, shib" within EBSCOadmin's "Customize Services" section for EBSCOhost databases and for EDS.[10]

Privacy Considerations Using this Method

As a result of working with platforms such as ACM Digital Library, where we were required to pull our SAML response using the https://dl.acm.org/action/showIdentities, we were able to confirm that this method of Shibboleth InCommon configuration does not release the end user's identifying information. We already assumed this was the case because we were relying on the "eduPersonScopedAffiliation" entity, but pulling this info through the "showIdentities" URL allowed us to investigate what specifically is being released. So while previous authors have raised concerns about identifying information being passed through Shibboleth authentication, we can confirm that this does not occur for our InCommon Shibboleth configuration (Kraft, 2019, p. 77). For platforms such as EBSCO which allow for personal accounts to be linked to Shibboleth authentication, this could be a concern, but in the case of EBSCO this is optional. Of all the platforms mentioned in the appendix for this study, EBSCO is the only one that allows for this feature; in all others, end-users' identifying information does not persist because of the entities being used.

Results & Future Directions

At the time of writing in December 2023, many of the Shibboleth configurations discussed in this paper have only been live for 4-5 months, and it is still far too early to tell what impact this has had on usage of our e-resources. At the same time, since going live, we have not experienced any disruptions to our access, and we see this as a positive sign. Having Shibboleth as an additional authentication method alongside EZproxy, rather than the sole method, has undoubtedly helped with maintaining access. For at least one vendor, EBSCO, we were able to track the authentication method of our users to see how many of them are using Shibboleth instead of IP authentication or EZproxy. While we have not been collecting this data long enough to draw conclusions, it will allow us to monitor usage patterns over time. For the majority of the other vendors listed in this article, the ability to track usage by authentication method is unfortunately unavailable, and as a result, it will be difficult to measure what impact this has had on usage. A different, less direct approach will be to simply observe how usage statistics change over the next year or so. While it will not be possible to determine whether any increase or decrease is attributable to Shibboleth authentication, it will provide some insight into whether this implementation facilitated greater and easier usage of our e-resources. Already, there have been a handful of resources which reflect a shift in usage patterns.

A unique early example where the change to Shibboleth could be measured almost immediately was presented by PubMed's "Outside Tool," where we were able to remove our EZproxy prefix, add

[10] Ironically, while we have yet to find a way to convert our OpenURL link structure to Shibboleth within the majority of databases, we have been able to use these configurations within EBSCOadmin to configure Shibboleth for PubMed's "Outside Tool" feature without having to use our EZproxy prefix. In this case, the database itself does not rely on Shibboleth, but instead, the EBSCO OpenURL links (the "Outside Tool" feature) incorporate the same "cookie, ip, shib" structure.

Shibboleth, and facilitate browser cookies. In short, "Outside Tool" allows for libraries to insert their link resolver into all of PubMed's article records (National Library of Medicine, 2023). In the context of UD, the link resolver is EBSCO's Full Text Finder (FTF), and UD has had this feature configured within PubMed for years. Until recently, we used the following url without any cookies and with our EZproxy prefix: **https://libproxy.udayton.edu/login?url=https://resolver.ebscohost.com/openurl?custid=s9003728&sid=Entrez:PubMed&id=pmid:**. Note that this does not include any of the "authtype" phrasing (as described in earlier sections) to route users to different authentication modes. We changed this url structure to allow for Shibboleth authentication to EBSCO's Full Text Finder link resolver from PubMed records using the following url structure: **https://resolver.ebscohost.com/openurl?authtype=cookie,ip,shib,uid,user,url&custid=s9003728&sid=Entrez:PubMed&id=pmid:**. This new structure tested successfully from off-campus, and we implemented the change over Thanksgiving break in November 2023. Crucially, the "shib" feature in the url allowed us to remove our EZproxy prefix from our custom PubMed link (https://pubmed.ncbi.nlm.nih.gov/?otool=ohudaylib) within our A-Z database list. Removing this and allowing for the "authtype=cookie,ip,shib" to function for authentication instead, enabled a major benefit for our off-campus users: it made the browser cookies for these resolver links within PubMed more effective than before for off-campus users. After the change went live, if a user first clicks the custom UD PubMed link containing UD's custom PubMed ID (https://pubmed.ncbi.nlm.nih.gov/?otool=ohudaylib) and clicks one of the EBSCO FTF links with Shibboleth authentication and cookies, they then have a cookie that will remember UD's Outside Tool links (for the 8 hours which PubMed cookies allow).[11]

These browser cookies in turn allow for users to select links to PubMed via Google and other search engines outside of the library website (i.e. without the "?otool=ohudaylib" URL suffix), while still having the UD Outside Tool links appear. This feature with the cookies for off-campus users is entirely dependent on Shibboleth authentication. When we tested the same workflow off-campus to see if a link relying on EZproxy without Shibboleth, but with the cookie authtype (specifically "authtype=cookie,ip,uid,user,url&custid=s9003728"), to see whether this url structure would still switch seamlessly between the UD proxied version of PubMed and the off-campus un-proxied version, we found that the UD Outside Tool links were not remembered. This difference would have a negative impact on usage for off-campus users.

In terms of results, usage within UD's instance of PubMed did seem to change significantly in the days after this switch was made, reflected by statistics provided by PubMed's admin interface for the tool. The results suggest that this link change for Outside Tool was at least partly responsible for a spike in our usage since it went live. Usage was consistently higher for nearly three weeks in a row following the launch, and the first 10 days in December were significantly higher when compared to November and September's usage. This was followed by low usage once UD's finals week ended in mid December. We plan to monitor this in 2024 to see if the usage continues to increase because as of December 2023 it is simply too early to tell.

A second example can be seen in Figure 9, where the admin dashboard for ScienceDirect displays a breakdown of on-campus vs. off-campus usage. Conveniently they break down the percentage of

[11] Note that 8 hours is unusually short for cookies; most platforms remember users for weeks and months at a time.

Federated Single Sign-On and “personalized usage”. Again, it is far too early to draw conclusions about usage trends, but the initial reports seem to indicate that users almost immediately started using Shibboleth. In the longer term, we intend to explore ways to track how many of our users are authenticating via Shibboleth vs. EZproxy for other platforms.

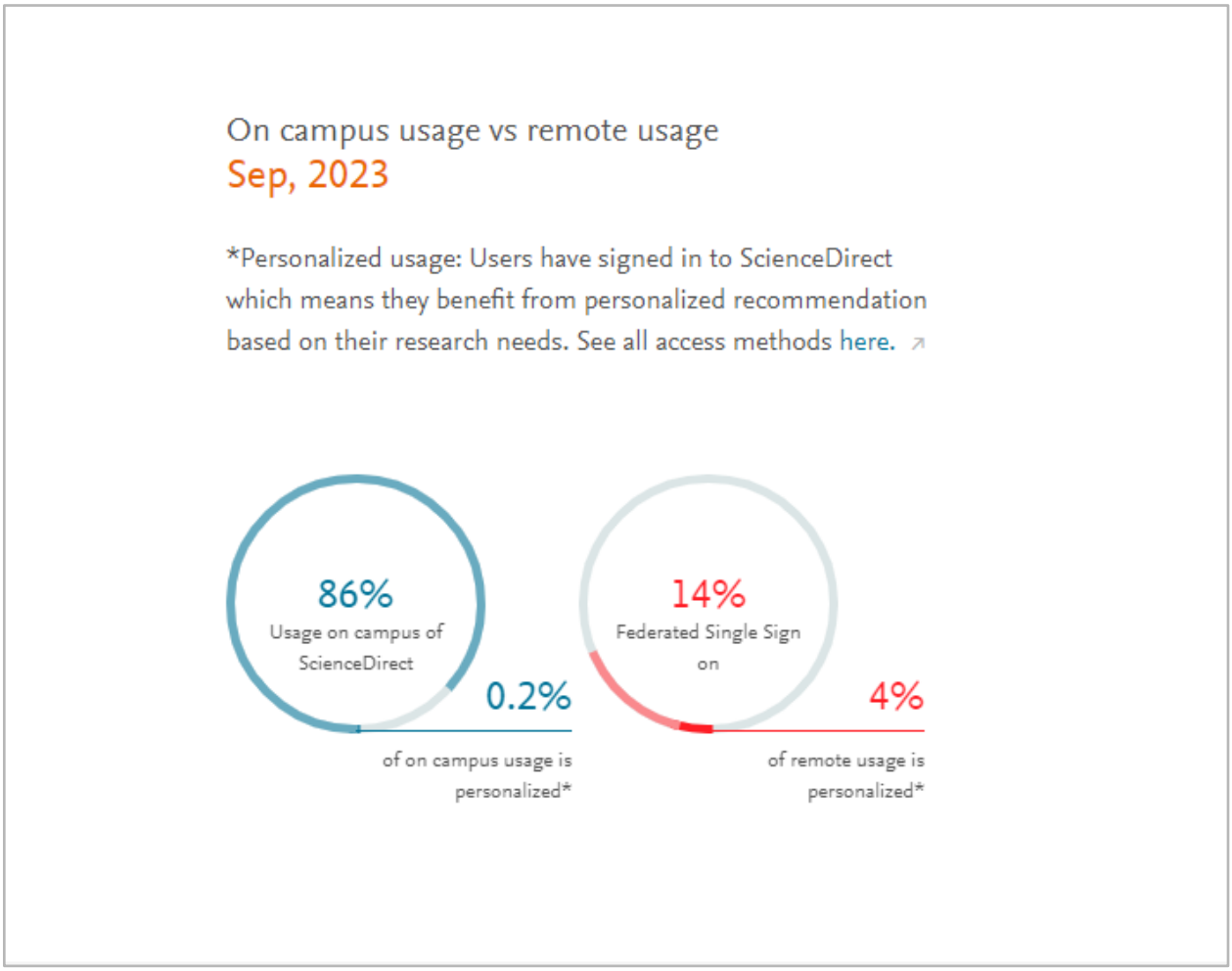


Figure 7. A report on usage of ScienceDirect from an admin account dashboard. Note how off-campus access via federated single sign on facilitates a more personalized experience, likely because users decide to create a personal ScienceDirect account when authenticating via Shibboleth.

Elsewhere, in terms of qualitative feedback, a demo of how Shibboleth authentication works was delivered to UD liaison librarians in mid-August 2023 and participants seemed excited by the opportunity for more seamless off-campus access for students and faculty who are primarily remote. Additionally, we have engaged with the EZproxy listserv to disseminate what we have learned, as many members of the e-resources community are confused about what to do in light of the looming browser changes. We have corresponded directly with several librarians at universities in Canada and the United States.

Lastly, in terms of usability of the Shibboleth authentication links on the public-facing websites, the majority of implementations are user friendly and adhere to the 2019 NISO standard and

SeamlessAccess Service's design recommendations, as depicted in Figures 4a and 4b. For a handful of other platforms,[12] the experience is cumbersome for the end user to select their federation. Specifically these platforms require the end user to select their federation, followed by their institution. From the authors' perspective, it seems unlikely that any undergrad will understand what "InCommon US" means within a dropdown menu to select the federation, and they will likely not know what to do. It seems imperative that these vendors improve the functionality.

Next steps

Due to the recency of implementation, we have multiple next steps. Plans are already in place to work with the Assistant Dean for Strategic Communication and Outreach to draft a blog post for UD's faculty and staff to explain how the new authentication method can benefit users whose experiences are impacted because of the browser privacy changes that mask their IP addresses. We plan to continue implementing Shibboleth for as many platforms as possible, using the process described in this article. We estimate that there are at least fifty additional subscriptions where this could be possible, and we are currently working with vendors to enable it for additional platforms. We will communicate to faculty and students about those platforms that do not allow for the "Access through your institution" method of authentication, and we will make them aware that they will need to authenticate by starting with the library website in such cases. One final adjustment we might make is with the platforms in which we have already configured Shibboleth. Most of the current platforms say "Access through University of Dayton." We feel this could be more specific and say "Access through University of Dayton Libraries," to provide the library with additional visibility to students and faculty.

Limitations

A key limitation of this report is the authors do not know the full extent of how the experience of Shibboleth authentication differs from authentication via OpenAthens. A future direction for this research would be to comprehensively compare an OpenAthens configuration of a database with a configuration of Shibboleth. So far as we are able to determine, the experience of using OpenAthens is highly similar to Shibboleth, with the key difference being that Shibboleth requires staffing within the library to configure and maintain the authentication mode, whereas OpenAthens outsources this responsibility to a third party.

Conclusions

In all, implementing Shibboleth was significantly easier than we expected it would be, but at the same time, we were made acutely aware of the lack of guidance on how to go about this implementation. It seems that the current understanding of Shibboleth configuration–from what we have witnessed on listserv discussions and in the absence of more recent publications–is now outdated. Many librarians seem to assume that implementing Shibboleth requires a laborious and time-consuming collaboration with the central IT office, similar to what this article describes for implementing SAML 2.0 for Safari.

[12] This includes AIP Publishing, Allen Press, American Physiological Society journals, ASME journals, Canadian Science Publishing, Company of Biologists, Duke Uni Press, geoscience world, Portland Press, Rockefeller University Press, U of California Press, and Web of Science.

Membership in an identity federation such as InCommon, coupled with its affiliation with the broader eduGAIN interfederation streamlines this process significantly. . The publishers themselves provide ample documentation of this within their public-facing websites, and a key question to emerge from our work in this area is: why has there not been more discussion within the e-resources community on this topic? For example, the screenshot in Figure 8 shows the public-facing web page from the publisher Optica, and earlier in this publication, we mentioned how EBSCO offers extensive documentation on how to enable Shibboleth. Clearly this documentation is not reaching the right audience within the LIS community and has not led to widespread implementations.

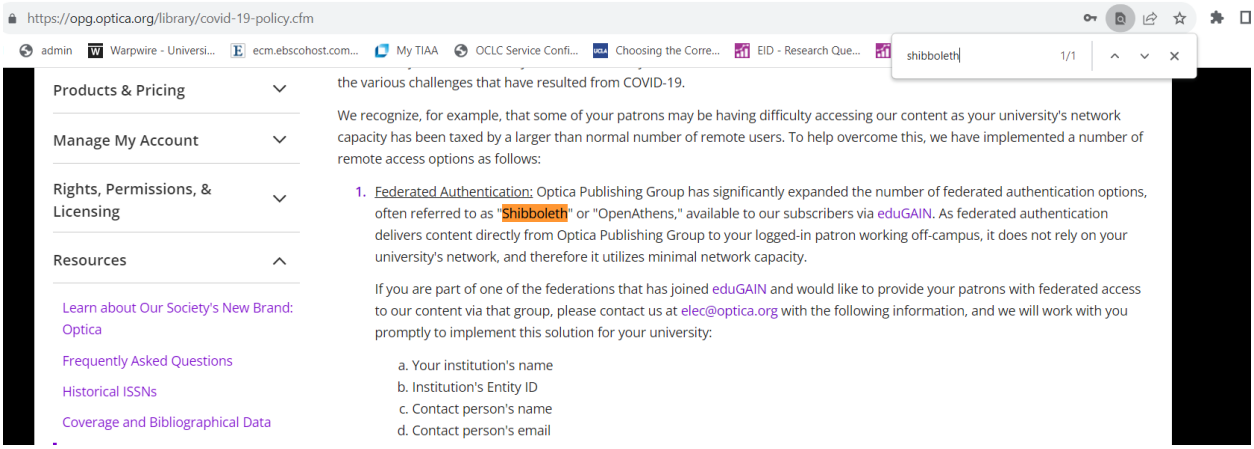


Figure 8.

This trend applies broadly. University of Dayton belongs to the OhioLINK consortium, and based on what we can publicly see from the dropdown menus for institutions (in platforms such as Wiley Online Library), at the time of writing (early December 2023), UD is one of only two OhioLINK institutions that have configured this additional authentication mode across a wide number of platforms (the other institution is Ohio University). This is also the case with Sage. The authors of this study were surprised by the relatively small number of institutions with Shibboleth configured across North America. This stands in stark contrast to European federations where there are hundreds of institutions listed. By way of comparison, even OpenAthens has few subscribers across OhioLINK institutions. So far as we can confirm, only two institutions within the entire OhioLINK consortium have OpenAthens. One of the authors of this study tried reaching out to OhioLINK to see if they wanted to lead their member institutions to implement Shibboleth as a way to offset the looming browser changes, but the consortium declined to take any action and confirmed that their stance concerning authentication configuration is for individual institutions to decide. The authors of this study agree with this stance in part. Institutions should decide on their own, and they should only make these sorts of changes when they are equipped and staffed to do so. At the same time, we are convinced that other OhioLINK members who belong to the InCommon authentication federation are simply unaware of how to turn Shibboleth on, and perhaps if they were made aware by OhioLINK leadership, they would choose to turn it on. This in turn would greatly benefit the end users at those institutions by making access more seamless, fitting within the vision that OhioLINK embraces in their 2020 White Paper (Evans & Schonfeld, 2020), and it would help mitigate the looming risk of browser privacy changes. More research is needed on institutions' awareness levels of what Shibboleth can do and how to turn it on.

This publication is an attempt to raise awareness of Shibboleth as an authentication method for any institution that is advantaged to turn it on. We aimed to present the process in a simple and straightforward manner. We also realize the phrase "any institution that is advantaged to turn it on" excludes a majority of academic libraries. For example, out of 117 OhioLINK member institutions, there are at most 15 institutions listed publicly within eduGAIN, the pre-requisite for turning Shibboleth on as part of InCommon. Meanwhile, there are hundreds of other universities across the country listed in eduGAIN who could benefit from turning on Shibboleth using the same methods discussed in this study.[13] So while this article does not apply to thousands of academic libraries, it still applies to hundreds. What the other institutions who do not belong to eduGAIN-affiliated federations would likely need is the financial support (and financial investment) from their institutions, likely via their central IT departments. We realize that this investment in the form of annual membership fees and additional staffing is likely a longshot given enrollment and budgetary challenges at many institutions currently.

Still, given the ample calls by the LIS community for the publishers to make access more seamless for the end user, in a way that cuts across different locations and moves with the user (Dempsey, 2020; Evans & Schonfeld, 2020; Lean Library, 2021), it seems that the LIS community (and/or the universities that fund and staff academic libraries) has failed in this instance to invest the time and resources to enable this authentication method. More specifically, the academic library community in the United States lags far behind those of other nations, specifically in Europe. Likewise the publishers could do more to train the institutions on how to configure this access, and they too could invest in greater staffing levels to support this configuration on their end, while also better adhering to the 2019 NISO standard when their platforms make it cumbersome for the end user to select their federation (NISO, 2019). This call for leadership, either from the publishers or from library organizations and consortia, rejects the notion that institutions should be left to fend for themselves to their own detriment.

Declaration of interest statement

The authors report there are no competing interests to declare.

References

Blankemeyer, B., Siler, L., & Tokoro, S. (2021). The New Frontier: Implementing OpenAthens at UNC Charlotte. *Serials Review*, *47*(1), 1–5. https://doi.org/10.1080/00987913.2020.1860431

[13] For example, through participation on the EZproxy listserv, in late August 2023, librarians at University of Prince Edward Island and the University of Michigan confirmed to one of the authors of this study that they were unaware of the straightforward nature of Shibboleth configuration.

Carpenter, T. A. (2019). Moving to a world of more seamless single sign-on access: NISO's RA21 Recommended Practice. *Serials Review*, *45*(3), 193–195. https://doi.org/10.1080/00987913.2019.1644843

Dempsey, Lorcan 2020. Foreword to resource discovery for the twenty-first century library: Case studies and perspectives on the role of IT in user engagement and empowerment, xxi–xxxii. Edited by Simon McLeish. London: Facet Publishing. OCLC Research Foreword Preprint. https://doi.org/10.25333/p8j4-1411

Dowling, T. (2020). We have outgrown IP authentication. *Journal of Electronic Resources Librarianship*, *32*(1), 39–46. https://doi.org/10.1080/1941126X.2019.1709738

Evans, G. & Schonfeld, R.C. (2020). *It's Not What Libraries Hold; It's Who Libraries Serve: Seeking a User-Centered Future for Academic Libraries*. Ithaka S+R. 23 January 2020.

EBSCO (2023). What to Know About Changes to Major Browsers: Top Eight Takeaways from ALA Annual. https://www.ebsco.com/blogs/ebscopost/2492355/what-know-about-changes-major-browsers-top-eight-takeaways-ala-annual

Hamparian, Don (2023, May 23). *Myths and Facts about EZproxy, FedCM, and Browser Changes* [PowerPoint slides]. https://www.oclc.org/content/dam/oclc/ezproxy/webinar/ezproxy-webinar-slides-myths-facts-23-may-2023.pdf.

Hanson, C. (2018, May 23). *In Defense of the Proxy Server* [PowerPoint slides]. https://www.niso.org/events/2018/05/digital-libraries-authentication-access-security-information-resources.

Herther, N. K. (2018). Resource access for the 21st Century: A new standard's rocky introduction. *Online Searcher*, *42*(6), 34–41.

Hoy, M. B. (2019). An introduction to RA21: Taking authentication beyond IP addresses. *Medical Reference Services Quarterly*, *38*(1), 81–86. https://doi.org/10.1080/02763869.2019.1554370

Janicke Hinchliffe, L. (2018, January 16). What will you do when they come for your proxy server? *The Scholarly Kitchen*. https://scholarlykitchen.sspnet.org/2018/01/16/what-will-you-do-when-they-come-for-your-proxy-server-ra21/

Jayakanth, F., Byrappa, A., & Visvanathan, R. (2021). Off-campus access to licensed online resources through Shibboleth. *Information Technology and Libraries*, *40*(2). https://doi.org/10.6017/ital.v40i2.12589

Jie, W., Arshad, J., Sinnott, R., Townend, P., & Lei, Z. (2011). A review of grid authentication and authorization technologies and support for federated access control. *ACM Computing Surveys*, *43*(2), 1–26. https://doi.org/10.1145/1883612.1883619

Kraft, M. (2018, April 27). Medlibs needs RA21 on their RADAR. *Krafty Librarian*. https://kraftylibrarian.com/2018/04/

Kraft, M. (2019). RA21 considerations for medical libraries. *Journal of Electronic Resources in Medical Libraries*, *16*(2), 75–80. https://doi.org/10.1080/15424065.2019.1638868

Lean Library. (2021). Librarian futures report. SAGE Publishing. https://doi.org/10.4135/wp.20211103

Li, H., Holly, C., & Goodrich, T. (2022). OpenAthens implementation: A two-phased move at our library. *Serials Review*, *48*(3–4), 201–205. https://doi.org/10.1080/00987913.2022.2106817

Lloyd, T. (2020). Introduction to SeamlessAccess. *Information Services and Use, 40*(3), 201-205. https://doi.org/10.3233/ISU-200091

M., M. T., Rao, M., & K., S. B. (2023). Enabling OpenAthens single sign-on (SSO) remote access authentication to e-resources: A case study. *DESIDOC Journal of Library & Information Technology*, *43*(5), 347–353. https://doi.org/10.14429/djlit.43.05.18872

National Information Standards Organization (NISO) (2019). *Recommended Practices for Improved Access to Institutionally-Provided Information Resources*. https://www.niso.org/publications/rp-27-2019-ra21

National Library of Medicine (2023). *Information for libraries*. https://www.ncbi.nlm.nih.gov/projects/linkout/doc/libraries.html

OCLC (2023). Will EZproxy be supported with the planned browser privacy features being introduced by Google and others. *OCLC FAQ*. https://help.oclc.org/Library_Management/EZproxy/Troubleshooting/Will_EZproxy_be_supported_with_the_planned_browser_privacy_features_being_introduced_by_Google_and_others

Palmer, R. (2019). *The GALILEO OpenAthens Project*. *56*.

Pawlowski, A., Beadles, M. (2018, May 23) *Authentication and access of licensed content in Ohio: A summary* [PowerPoint slides]. https://www.niso.org/events/2018/05/digital-libraries-authentication-access-security-information-resources.

REFEDS Browser Changes and Federation Working Group (2023, September 29). *Browser Changes and Federation*. REFEDS Wiki. https://wiki.refeds.org/display/GROUPS/Browser+Changes+and+Federation

Ruenz, M. M. (2022). Remote authentication: One library's journey on offering EZproxy and OpenAthens. *Internet Reference Services Quarterly*, *26*(3), 153–167. https://doi.org/10.1080/10875301.2022.2067283

Schmidt, L. M. (2011). ILLiad, CAS, Shibboleth, and PHP: The road to single sign-on. *Journal of Interlibrary Loan,Document Delivery & Electronic Reserve*, *21*(3), 149–156. https://doi.org/10.1080/1072303X.2011.585280

Schwing, T. (2018, May 23). *Challenges to successful authentication change: Barriers for libraries based on institution size* [PowerPoint slides]. https://www.niso.org/events/2018/05/digital-libraries-authentication-access-security-information-resources.

SeamlessAccess (2023, November 16). *Third-party cookie deprecation and its effect on SeamlessAccess*. SeamlessAccess.org. https://seamlessaccess.org/posts/2023-11-16-3pp-cookies-and-the-sa-button

Seguin, J. (2019). The future of access: How a mosaic of next-gen solutions will deliver more convenient access to more users. *Information Services & Use*, *39*(3), 237–242. https://doi.org/10.3233/ISU-190049

Tay, A. (2022). Chapter 6. Improving access to and delivery of academic content from libraries: A roundup. *ALA TechSource*. https://journals.ala.org/index.php/ltr/article/view/7853

Zhu, J. (2023). Implementing and assessing SeamlessAccess: A publisher's perspective. *Information Services & Use, 43*(3-4), 311-322. https://doi.org/10.3233/ISU-230203

Appendix I – List of platforms with Shibboleth turned on University of Dayton (so far)

1. AAAS Science
2. ACM
3. ACS
4. AIAA subscriptions
5. AIP

6. AllenPress
7. American National Biography Online (Oxford)
8. American Physiological Society journals
9. ASCE
10. ASM microbiology journals
11. ASME journals
12. Brill
13. Cambridge Core
14. Canadian Science Publishing
15. Company of Biologists
16. Duke Uni Press
17. EBSCO
18. Emerald
19. Gale/cengage
20. Geoscience world
21. Guilford University Press
22. IEEE Xplore
23. IOP Science
24. JAMA
25. JSTOR
26. Microbiology Society
27. MIT Press E-books (MIT Press Direct)
28. Nature.com
29. New England Journal of Medicine
30. OPTICA
31. Ovid
32. Oxford Academic
33. Oxford African American Studies Center
34. Oxford Art Online
35. Oxford English Dictionary
36. Oxford Music Online
37. Oxford Research Encyclopedias
38. PNAS
39. Portland Press
40. Project Euclid
41. Project Muse
42. Psychiatry Online
43. Rockefeller University Press
44. Routledge Encyclopedia of Philosophy
45. Sage Business Cases
46. Sage Data
47. Sage Journals
48. ScienceDirect
49. SPIE

50. SpringerLINK
51. Taylor & Francis Online
52. U of California Press
53. U of Chicago Press
54. Web of Science
55. Wiley Online Library

Appendix II – SAML attributes released for ACM digital library– Simon Robins logged in via Shibboleth to generate these–nothing is generated about identity:

```
<saml2:AttributeStatement>
        <saml2:Attribute FriendlyName="eduPersonScopedAffiliation"
                Name="urn:oid:1.3.6.1.4.1.5923.1.1.1.9"
                NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
        <saml2:AttributeValue>FACSTAFF@udayton.edu</saml2:AttributeValue>
        <saml2:AttributeValue>FACULTY@udayton.edu</saml2:AttributeValue>
</saml2:Attribute>
<saml2:Attribute FriendlyName="eduPersonEntitlement"
                Name="urn:oid:1.3.6.1.4.1.5923.1.1.1.7"
                NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
        <saml2:AttributeValue xmlns:xsd="http://www.w3.org/2001/XMLSchema"
                xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
                xsi:type="xsd:string">urn:mace:dir:entitlement:common-lib-terms
</saml2:AttributeValue>
<saml2:AttributeValue xmlns:xsd="http://www.w3.org/2001/XMLSchema"
        xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
        xsi:type="xsd:string">urn:mace:incommon:entitlement:common:1
</saml2:AttributeValue>
</saml2:Attribute>
</saml2:AttributeStatement>
```