UKSG webinar Q&A

‘Federated authentication for library resources: can it be trusted?’

Lee Houghton | Heather Flanagan | Jos Westerbeke | Kelechi Okere

Questions that came during the presentation:

“Q: How will the changes to browsers and operating systems defaulting to VPN-like hiding of IP addresses affect those that continue to rely on IP-based authentication? (Apple will launch this in September on Mac and iOS)”

- **Heather:** I think they will still have difficulties, based on what Apple has said in their WWDC’21 announcement: “Private Relay is a new internet privacy service that’s built right into iCloud, allowing users to connect to and browse the web in a more secure and private way. When browsing with Safari, Private Relay ensures all traffic leaving a user’s device is encrypted, so no one between the user and the website they are visiting can access and read it, not even Apple or the user’s network provider. All the user’s requests are then sent through two separate internet relays. The first assigns the user an anonymous IP address that maps to their region but not their actual location. The second decrypts the web address they want to visit and forwards them to their destination. This separation of information protects the user’s privacy because no single entity can identify both who a user is and which sites they visit” -- https://www.apple.com/newsroom/2021/06/apple-advances-its-privacy-leadership-with-ios-15-ipados-15-macos-monterey-and-watchos-8/

“Q: Technically, is authentication access for user granted through multiple devices & platforms?”

- **Heather:** I’m not entirely sure about the question, but I think you’re asking if a user has to authenticate separately for each device and platform. If that’s a correct interpretation, then yes. The user will have to authenticate per platform, per device.

“Q: Does it matter if we use OCLC ezproxy?”

- **Jos:** When browsers hide their IP address, the EZproxy server cannot see the IP address of the user, but the user can still authenticate to the EZproxy server, and the EZproxy server does not hide its IP address to the Service Provider/e-resource website. So, it still works. But then, you always must authenticate to EZproxy because the EZproxy server does not see whether

you're on- or off-campus. For browsers hiding their IP address, EZproxy will be the only solution to provide access to resources relying on IP address recognition.

"Q: Can seamless access totally replace proxy access? What about when a provider doesn't offer institutional access, wouldn't you still need proxy access?"

- **Heather:** We're going to see proxy access as an option for a very long time. Smaller publishers and smaller institutions both need time to be able to build up their infrastructure to support federated identity.

- **Lee:** The issue with some providers is that institutional access is not uppermost in their minds as their main customer base is corporations and other types of organisations instead. So, they don't have as much incentive to adopt federated authentication and continue to offer username/password or just IP authentication instead. If federated auth gains traction with more than just educational institutions this might force some changes that have a wider reach.

"Q: Any suggestions for working with librarian colleagues who have dismissed Fed Auth due to deep seated suspicions about personally identifying data leaking out and/or about service providers eventually planning to end IP access and cut out library guest access?"

- **Kelechi:** Based on how other libraries have handled it, my suggestion would be to schedule a meeting with your IT and invite those library colleagues to discuss attribute release. Part of the suspicion comes from lack of understanding of attribute release since it's out of the domain of the library. So, help them get educated about it. I would also recommend asking a peer library that uses federated access to talk to your library about it.

"Q: When we go to eBook publisher's website, they always insist that we choose our institution from a list. Rather than admitting that we have access to a title they ask for more information, which institution are you from? This is despite us being signed in with an authentication provider. they are not asking, nor do they need personal information and yet they also don't admit that an institution has access to a title. does the panel know why this is so?"

- **Kelechi:** It's hard to answer this question since it's possible none of us works for the e-book publisher in question. In general, with federated access, authentication and authorization are two separate functions/steps. When a user first logs in, in this case, the authentication provider authenticates the user as being who they say they are. But in order for the publisher to

authorize access to the subscribed e-books package of the user's institution, the publisher needs to ask the institution's Identity Provider (IdP) to validate that the authenticated user is an authorized user of the institution's subscriptions. This could be why the publisher insists that you choose your institution from a list.

"Q: We have a service provider that uses library members' email addresses to personalise services and save video playlists, this is asked for in a separate step after initial login with federated authentication. Would the service provider switching to privacy-preserving option, would it mean existing users losing their personalised content?"

- **Heather:** Many service providers use federated authentication purely as a mechanism to ensure that the user is the same user from a given institution each time they log in, and then ask for additional information such as name and email to 'decorate' the account with more detail. I don't see service providers changing that behavior any time soon, as it gives them some measure of control over whether the user consents for the service provider to have that information. When the consent options happen entirely out of the service provider's perspective, they get nervous that they might be held accountable if the institution releases more information than the user is willing to share.

"Q: (Sorry for newbie question..) Are Shibboleth and OpenAthens considered to be federated authentication systems?"

- **Heather:** This is a great question, actually! The answer is "yes, and". Shibboleth is an open source software product that is used to run federated authentication system. What OpenAthens is depends on the context – OpenAthens is a federation. OpenAthens is also a company. And, just to complete the confusion, OpenAthens as a term is often used to describe one of several products offered by that company (including an Identity Provider service and a proxy service). But to simplify, whereas Shibboleth is designed to run a federated authentication system for several applications at an organization, OpenAthens is designed to run federated authentication specifically for library e-resources.

“Q: How does federated search compare to EZproxy services such as OCLC? We currently use SAML based SSO but all resources must be accessed via the library website/link to them. So if one of our patrons went to Science Direct via a google search (not our discovery service) our institution does not appear as an option on the "what institution do you belong to" on Elsevier's list. Should we be doing something differently?”

- **Kelechi:** The possible reason for this is that Elsevier doesn’t yet have your IdP metadata in its SP. Go here for some instructions of what to do and who to contact at Elsevier to resolve this issue.

“Q: I just logged on to ScienceDirect via Seamless Access. Then I was presented with a prompt to optionally log in with my individual user account. Would Elsevier then link my individual user info with my SA login info?”

- **Kelechi:** Yes, this is possible if you want to associate your individual user account with your institutional login. This helps to personalize your experience every time you use ScienceDirect. The Elsevier Privacy Center helps give you control over your data.

“Q: Are there any disadvantages to using a proxy service (e.g. hosted EZproxy from OCLC) to manage both on-campus and off-campus use?”

- **Kelechi:** One reported disadvantage is that the on-campus login discourages users and results in drops in usage. You can talk to the COUPERIN Consortium in France about their experience with this.

- **Jos:** Another disadvantage could be that not all of your licensed websites work through EZproxy.

“Q: Some providers will not enable federated access without email and/or name..or forcing user registration. What can we say to them when the resource is essential reading?”

- **Kelechi:** Generally, federated access technology does not require email and/or the users name to work. Users can be authenticated anonymously. You have leverage as a customer to force the provider to drop that requirement.

- **Jos:** You may use FIM4L recommendations when you negotiate with your provider. These are supported by library associations like LIBER, CARL, CAUL, RLUK.

“Q: For academic libraries that wish to correlate usage of electronic usage with schools, colleges, departments, etc., for budgetary or training purposes (reaching the users who interact with the vendor product), are there ways for the library to get this kind of user data?”

- **Kelechi:** You’re referring to what is called granular usage reporting. It is possible with federated authentication but a provider would have to build it. Elsevier is now working on this and are actively gathering requirements. So please email Kelechi Okere at k.okere@elsevier.com if you’re interested in helping with the requirements gathering and subsequent pilot testing.

- **Jos:** In this case you (IdP) need to share some more user attributes besides the (pseudonymous) ID, like which faculty or department a user belongs to.

“Q: I am finding that increasingly providers are asking for attributes which they claim facilitate personalisation- not much choice on our part- give us the email address or you cannot access the resource- all dressed up as improved UX”

- **Heather:** Yes, this is a common pattern, though they really need to offer a choice. Personalization should never be required to have a site function. It is a nice to have, not a need to have.