Mobile authentication and access: any time, any place, any device?

The move from IP-based authentication to that of federated access has seen the sector support single sign-on to web-based resources, but the simplified user experience is at risk due to the rapid growth of mobile platforms and increasing variety of accompanying access methods for such devices. The user authentication experience on mobile devices is often further complicated by the poor discovery and delivery design of websites. While the introduction of tools such as Raptor permit accurate tracking of usage statistics via the UK Access Management Federation, the variety of mobile authentication methods such as native apps on devices and device paring pose additional challenges to librarians trying to gather a complete picture of resource use within their institution. In this article we examine the access challenges posed by the explosion of mobile device use.

The story so far

MARK WILLIAMS
Operator Manager
UK Access Management Federation
JISC Collections

Over the last five years, we have seen the UK education sector move from proprietary, password and IP-based authentication systems for accessing content to one built around the federated identity management model[1], where multiple organizations use the same data standard to gain access to services within a managed trust fabric. This change has meant that institutions and resource providers can choose whether they go down the route of using their own standards-based, non proprietary SAML[2]-based solutions (most commonly in the UK HE sector, Shibboleth[3]) or using third-party services (themselves incorporating SAML standards for true interoperability, such as OpenAthens[4]). The enabling of institutions to have full control of their own access management structures has permitted a move to a single sign-on environment – ideally linking the user seamlessly with the institution network, learning environment, internal management systems and web-based subscription resources.

At the same time, we have steady improvement in the quality and range of resources available online.

Parallel to this, there has been an explosion in the market of mobile devices capable of accessing and consuming online resources. A recent report by Flurry, which specializes in analysing web market share, stated,

'Smart device adoption is being adopted 10X faster than that of the 80s PC revolution, 2X faster than that of 90s Internet Boom and 3X faster than that of recent social network adoption.'[5]

Freed from a ten-kilo desktop PC, users have a variety of mobile devices to suit their needs, which, when coupled with non IP-based, federated access provided by their institutions, should enable any time, anywhere, any device consumption of content.

How the sums really add up

The user equation of access should run something like this:

federated access + mobile device = any time, anywhere consumption. This meets the requirements identified by the JISC Collections UBIRD study[6], which argued for the removal of as many barriers to access as possible so users find it easy to use trusted subscription resources and therefore not take the path-of-least-resistance route, which can be Wikipedia

and its kin. Sadly, this equation is not always correct. The 'discovery to delivery' process as defined by NISO[7], which has developed a set of excellent single sign-on recommendations for publishers, poses significant challenges to the user wishing to access and authenticate to online resources in a mobile environment.

The typical experience

"The 'discovery to delivery' process … poses significant challenges to the user wishing to access and authenticate to online resources in a mobile environment."

For some time now, resource providers and institutions have been converging on a single set of standards, promoted by JISC Collections within its licensing deals that permit federated access via the UK access management federation. Resource providers, in their understandable urge to meet the new requirements of users accessing content through mobile devices, have begun to diverge from this, with the development of mobile applications (apps).

Resource providers have two non-exclusive routes that they can go down when developing their content to suit mobile access.

The first is to develop a 'mobile site' which recognizes that the accessing device is using a mobile browser and subsequently provides the content in a format more suited to smaller screen, reduced user input, lower bandwidth scenarios. You can see this by visiting the websites of either of the top two free-to-access UK daily broadsheets, using a standard PC browser and then a mobile device. Librarians wishing to road-test the experience users might have on a range of mobile devices might like to try Firefox extensions, which will simulate a range of common mobile browsers, or some of the device-specific emulators[8].

The second is to develop an app, which is often platform-specific (a native app) and may utilize unique capabilities of the accessing smartphone, such as geo-location.

The problem is that unlike many of the non-educational apps available which can be bought and paid for in the two most used app marketplaces[9], the publisher is usually not making income on the app itself but on the subscriptions to the content on their site. This is where the importance and manner of access and authentication become significant.

The following scenario may be familiar:

The website says: '*Welcome to XXXX. We've spent a lot of time and effort optimizing our content so you can read it on a plethora of devices … and have developed this handy app…'*

The user thinks: *"Well, that's great. I've got an Android phone and I'm on the bus and have a great 3G connection via my superb network provider and I know my institution subscribes to this resource, so let's view or download an article to read."*

The problem is that the user then encounters this message:

'Access via this app is IP only – connect to your campus'

"But I'm mobile", says the user, *"I'm not on campus. I want mobile institutional access."*

"The time when a user is most likely to want mobile access is the very time they are most likely to be away from the physical campus."

While it is encouraging that resource providers are looking to cater for mobile use, it clearly breaks the federated model to which the sector has moved in order to ensure access off-campus. The time when a user is most likely to want mobile access is the very time they are most likely to be away from the physical campus. Some institutions will have proxy solutions that may help, but it is far from ideal.

A number of publishers provide the ability to enable account linking. This entails obtaining a token gained through an institutional log-in experience (either on or off campus via federated access) and then using that token when accessing the site via the app, which then

links the account and can enable instant click-through access for as long as the resource provider has selected, which can range from two hours to six months.

However, many apps sidestep the issue of having a genuine mobile authentication process to access resources by only allowing search and discovery and not content access, which has to be done via traditional browsers. This is clearly a pragmatic way for a publisher to ensure that they have an app catering to mobile access on offer, but falls short, providing *discovery* but not the *delivery* that users require.

"Apps can also pose challenges to how both libraries and publishers measure resource use."

Publisher-specific apps also start to break the preferred discovery process of institutional libraries, which when using discovery tools such as Summon[10], surface suitable content from a range of resource providers, thereby allowing the user to narrow the discovery field according to their own criteria. Using a specific app provided by a single publisher instantly narrows this field before any search results are returned. This is good for the resource provider hoping to offer the ubiquitous 'one-stop shop' but a poor experience for the student or researcher looking for a more catholic selection of resources. Lessons learned from the UBIRD study show that even that quick win for the publisher may only offer benefit to the publisher in the short term as the user, when faced with a failure to find what they want, may abandon the use of licensed resources as a whole.

Apps can also pose challenges to how both libraries and publishers measure resource use. Raptor[11] is a tool developed by JISC that provides detailed statistics on the number and nature of authentications taking place via federated access at an institution. Native mobile-based apps will frequently sidestep federated or institutional portal access, which will make gathering a complete picture of usage statistics problematic. Clearly, at a time when justifying resource purchase via usage statistics is becoming ever more important, an inability to record the quantity of individual resource authentications via mobile apps significantly undermines a library's ability to base purchase decisions on usage. Mobile usage statistics are not currently (at time of writing in September 2012) available via COUNTER. However, COUNTER release 4 will include them, although it remains to be seen if this will always include access via apps rather than through a mobile browser. Native apps also demonstrate a bias towards the market-leading mobile devices, forcing libraries to make difficult decisions rather than being technologically agnostic when it comes to platforms and devices.

Mobile browser problems and solutions

If using a publisher app often means a user is unable to utilize their institution's subscriptions directly, then the alternative method of access is obviously the browser-based one. Institutional sign-on to resources, although relatively straightforward on a normal-sized laptop, poses significant challenges when effected on a smaller mobile device such as a smart phone. If a user comes to a site at the landing page, they will choose the institutional login route and then either use the publisher's 'Where are you from' (WAYF) service to select their institution (often a pick-list limited to the resource's subscribing institutions) or the UK federation Central Discovery Service (CDS) and then be directed to their institution's single sign-on web page. Choosing from very long pick-lists and typing long institution names into text fields can be laborious when done on mobile devices, so the JISC Data Centre, EDINA, has improved the usability of the UK federation's CDS by incorporating both type-ahead technology and the use of 'MDUI' data[12]. Assuming that both the institution and the publisher have provided the UK federation with their respective branding and logos (the critical element of MDUI data), then each time the user visits the WAYF using the same browser, they will see the logos of both the institution from which they typically access resources and the resource provider they wish to access. This removes the need to type anything and maintains the continuity of the authentication journey. Resource providers who run their own WAYF can also download the relevant code and utilize this technology.

Additionally, institutions can play their part in developing their single sign-on portals with mobile browsers in mind, of which Glasgow University[13] is an excellent example. Keren Mills of the Open University in her MACON project[14] argues that students want Google functionality and therefore libraries should develop their portals with mobiles as a design priority.

Another tool that can ease the authentication headaches on a mobile device is the use of WAYFless URLs. These can remove a couple of the discovery and authentication steps that can be tricky on mobile devices. Although maintenance of a collection of WAYFless URLs can pose workload challenges to an institutional library, JISC is developing a tool named WUGEN[15] to help easily craft and improve the accuracy of WAYFless URL creation. The UK federation is looking to roll out the tool later in the year (2012) and welcomes feedback from anyone who wants to test the development version.

"… institutions can play their part in developing their single sign-on portals with mobile browsers in mind …"

Mobile authentication does not just bring new problems, but also tends to amplify the issues inherent in websites that already have poor 'discovery to delivery', which traditional laptop users frequently encounter. An example of this is when the user follows a direct link – from a virtual learning environment (VLE), reading list, RSS feed, social networking tab, etc. – finds themselves tantalizingly close to the content, is then asked to sign in and authenticate, and is finally taken on a convoluted journey that returns them back to the index page of the resource provider. This leaves them now authenticated, but lost as to the location of the content at which the link was originally targeted. This is a poor process, even for a desktop user who can easily switch back and forth between continually open browser windows displayed on a large monitor. It becomes exponentially more difficult for those using a mobile device with all the problems associated with having multiple applications and tabs running at the same time on a small, limited RAM mobile device such as a BlackBerry. The utility gained from direct linking to resources via social media, Facebook, Twitter, etc., so valuable to both educators and peer groups, is also significantly undermined.

As with apps, many resource providers are enabling device-twinning for mobile browser access, which effectively links an institutional user account with a specific device for a predetermined length of time. Publishers are also providing more opportunity for content download that can be viewed offline on devices such as the Kindle. This can be particularly valuable, as users tend to need to access content on mobile platforms when wireless and network coverage may be intermittent or unavailable.

The way ahead

Feedback from librarians to whom JISC Collections have spoken makes it clear that mobile access is something still in development, and it is evident that publishers are developing apps at a rapid pace, but one which has yet to match up with institutional access methods.

"This leaves them now authenticated, but lost as to the location of the content at which the link was originally targeted."

Development of apps by publishers is a direct response to technological change – adoption of smartphones is occurring at a more rapid pace than even PC adoption in the 90s[16]. However, the sector needs to play its part in clearly articulating the requirements of users to publishers and defining some of the constraints on institutional access that exist with current subscription models. Librarians themselves are still trying to understand mobile access patterns and experiences, so it is no wonder that publishers are finding it difficult to respond to user needs that are not yet fully realized and articulated.

Projects such as JISC Mobile libraries[17], and events such as the Mobile Libraries Conference[18] are certainly a start in collating information on these requirements, and JISC Collections is working to ensure that publishers with JISC Collections content deals provide as much

information as possible up front on the capabilities of their mobile access routes. Value-added extras, such as apps, do have an impact on other authentication routes and need to be considered as part of the whole, offering more than just a stand-alone silo of *nice to have*.

We should be seeing the realization of the promise of seamless access to subscription resources, with no technological impediments. Instead however, we are facing an entropic drift towards a chaotic diversity of access methods rather than the standards-based convergence point towards which we all thought we were heading.

"… we are facing an entropic drift towards a chaotic diversity of access methods …"

References and notes

1. Federated Identity
   UK Access Management Federation:
   http://www.ukfederation.org.uk/content/Documents/HowItWorks (accessed 28 September 2012).
2. SAML V2.0 Executive Overview, Ed: Madsen, P (NTT), Maler, E (Sun Microsystems); Contributors: Wisniewski, T (Entrust), Nadalin, T (IBM), Cantor, S, (Internet2), Hodges, J (Neustar) and Mishra, P (Principal Identity):
   https://www.oasis-open.org/committees/download.php/13525/sstc-saml-exec-overview-2.0-cd-01-2col.pdf (accessed 28 September 2012).
3. Shibboleth
   Shibboleth Consortium:
   http://shibboleth.net/about/index.html (accessed 28 September 2012).
4. OpenAthens
   JISC Monitoring Unit
   http://www.jiscmu.ac.uk/services/view/17 (accessed 28 September 2012).
5. Farago P, 27 August 2012, Flurry blog:
   http://blog.flurry.com/bid/88867/iOS-and-Android-Adoption-Explodes-Internationally (accessed 28 September 2012).
6. JISC user behaviour observational study, *User behaviour in resource discovery*, Wong, W, Stelmaszewska, H and Barn, B, Interaction Design Center; Bhimani, N, Learning Resources, Middlesex University Business School; and Barn, S, Middlesex University, 2010, London, JISC.
   http://www.jisc-collections.ac.uk/Global/ubird-report-final.pdf (accessed 28 September 2012).
7. *ESPReSSO: Establishing Suggested Practices Regarding Single Sign-On*, NISO Baltimore, Maryland USA, October 2011.
   http://www.niso.org/publications/rp/RP-11-2011_ESPReSSO.pdf (accessed 28 September 2012).
8. Android:
   developer.android.com/sdk/index.html (accessed 28 September 2012).
   Apple Iphone emulation software:
   http://iphone-emulator.org/ (accessed 28 August 2012).
   BlackBerry
   https://bdsc.webapps.blackberry.com/html5/download (accessed 28 September 2012).
9. Most used app marketplaces:
   http://www.forbes.com/sites/darcytravlos/2012/08/22/five-reasons-why-google-android-versus-apple-ios-market-share-numbers-dont-matter/ (accessed 19 October 2012).
10. Summon
    SerialsSolutions:
    http://www.serialssolutions.com/en/services/summon/ (accessed 28 September 2012).
11. Raptor is a software suite for accounting of authentication information, primarily designed to assist organizations account for e-resource usage:
    http://iam.cf.ac.uk/trac/RAPTOR (accessed 28 August 2012).
12. Metadata extensions for log-in and Discovery User Interface (MDUI) UK Access Management Federation:
    http://www.ukfederation.org.uk/content/Documents/MDUIRecommendations (accessed 28 September 2012).
13. Glasgow University mobile services:
    http://universityofglasgowlibrary.wordpress.com/2011/07/06/library-services-for-your-mobile/ (accessed 28 August 2012)
14. Mills K, 27 August 2012 M libraries blog:
    http://www.m-libraries.info/tag/macon/ (accessed 28 September 2012).
15. WUGEN link
    WAYFless URL Generator (Wugen):
    http://iam.cf.ac.uk/trac/wugen (accessed 28 September 2012).
16. Farago P, 27 August 2012, Flurry blog:
    http://blog.flurry.com/bid/88867/iOS-and-Android-Adoption-Explodes-Internationally (accessed 28 September 2012).
17. M libraries:
    http://www.m-libraries.info/2012/08/10/which-library-content-providers-are-utilising-mobile-technologies/ (accessed 28 September 2012).
18. Mobile Libraries Conference:
    http://www.m-libraries.org/news/online-sessions (accessed 28 September 2012).

Mark Williams, Operator Manager, UK Access Management Federation
JISC Collections, Brettenham House, 5 Lancaster Place, London WC2E 7EN, UK
Tel: +44 (0)2030066042 (Direct) ; Tel:+44 (0)2030066086 (Federation Support)
E-mail: m.williams@jisc-collections.ac.uk

To cite this article:

Williams, M, Mobile authentication and access: any time, any place, any device?, *Insights*, 2012, 25(3), 268–273, doi: 10.1629/2048-7754.25.3.268

To link to this article:

http://dx.doi.org/10.1629/2048-7754.25.3.268