

Would you eduID? Improving the user experience of federated access management

New technologies bring new challenges. Nowhere is this more applicable than the rollout of federated access management in the scholarly publishing world. The UK Access Management Federation for Education and Research has been successful in recruiting publishers across the board, with recent announcements of compliance from IEEE and Wiley completing the picture for many institutional resource portfolios. However, the widespread implementation of the standards-based approach to access management has given rise to a very specific problem – what do we call this thing we've started?



NICOLE HARRIS

Services Manager
JISC Executive

Background

The UK Access Management Federation for Education and Research¹ (the UK federation) was launched in November 2006. Based on the SAML² standard for access management, the UK federation was founded on the principles of changing the access management landscape within UK colleges and universities from one predominantly based on proprietary systems to one with open standards at its core. The aims of the transition to federated access management are to:

- improve the business decisions made by institutions and service providers in relation to identity, access and resource management
- increase the choice of access management software available to institutions and service providers
- reduce the impact and cost of vendor lock-in.

To meet these aims, the UK federation allows both publishers and institutions to have a choice of the access management software they use. Whilst most chose either the open-source Shibboleth³ software or the fully supported OpenAthens⁴ product, there are a range of other software implementations including Guanxi⁵, OpenID⁶, SimpleSAMLphp⁷ and the Atypion SAML SP⁸ software. The ability to have a choice of standard approaches is one of the

main benefits of the federated access approach in the UK. It has helped us move away from the 'one size fits all' approach to access management and means that both institutions and publishers can decide to change the software they use in the future with minimal disruption.

Most importantly, the federated access approach allows students and staff to use their institutional username and password to access scholarly resources. Not only does this simplify the number of credentials that users have to remember, it provides a much more secure environment by relying on a username that users are likely to closely protect and by not passing personal information across to publishers unless there is a perceived need for this exchange.

Are you going to go my WAYF?

Whilst increase of choice is a clear benefit for all of those involved in using access management systems, the change has introduced a complicated array of new terms and names that need to be navigated. What is federated access management? What is Shibboleth and is it different from SAML? Is this the same as single sign-on? What

should we tell users to look for on publisher websites?

An additional issue with the federated access approach is the introduction of the 'Where are you from' (WAYF) process. In order for publishers to allow users to enter their institutional username and password they need to ask 'Where are you from?' This process results in a visually unpleasing long list of all of the institutions involved in the UK federation and a poor user experience. Strategies for dealing with this have been put in place, such as the use of 'WAYFless' URLs within library portals which take users directly to the institutional log-in screen. This does not, however, help users accessing resources from other routes – such as a direct Google search. This conundrum is known as the 'discovery problem' for federated access management.

What's in a name?

Choice, while providing many benefits to adopters of federated access management, brings with it an amount of confusion about the best way to label the log-in process. Should it be labelled 'Shibboleth' to match the Athens logo that users are familiar with? Should it be called 'federated log-in', 'institutional log-in', 'UK federation access' or 'organizational log-in'?

To help manage this proliferation of names, JISC issued an advisory to publishers and other service providers on naming conventions – recommending that the term 'institutional log-in' be used to identify the federated log-in process. However, a couple of years into the rollout it is clear that this recommendation is not being followed and that a range of different terms are being used. This causes confusion for end-users and more work for librarians as they attempt to document the different terms and provide explanatory notes for all of the different access routes. Clearly, this problem area needs a resolution.

I'd like to teach the world to sing ...

A further area of interest for federated access management is the international engagement in the SAML standard. There are now over 25 access management federations throughout the world all using the same standard approach, which opens

up fantastic opportunities for collaboration. However, most of these federations are giving publishers slightly different advice as to the wording they should use to describe federated access to end-users. This is made more complex for publishers that are dealing with multiple federations and have to manage the WAYF process for both country and institution within that country. This creates multiple tiers of drop-down menus that users have to navigate. Harmonization across the access management federations can only improve this situation for publishers, institutions and users.

In order to get a clear picture of the extent of the log-in problem, JISC funded JISC Collections, Cardiff University and Kidderminster College to undertake a Publisher Interface Study⁹. The aims of the study were clear: to provide a snapshot of the extent of the problem through an analysis of publisher interfaces, to make recommendations for improving the discovery process for users and to gain international consensus across access management federations on a solution. The study examined a full range of resources, from large publishers dealing with multiple federations, to small society publishers and those offering specialist resources to Further Education colleges. Whilst a lot of good practice was identified, many confusing interfaces and contradictory terms and directions were found. Interestingly, the study also identified a lot of inconsistencies relating to access problems that are not directly associated with federated log-in – such as the fact that many publishers do not clearly identify when a user is logged in via IP address. Examples of publishers applying the wrong IP range to the wrong institution were also found, with some users being told they were logged in as institution X, when they were sitting in the library at institution Y.

The solution?

The Publisher Interface Study came up with a clear and simple proposal for improving the log-in process in two parts:

- Brand should be created for academic federated access. For this brand to be successful, it needs widespread adoption worldwide. The brand should include a short name and a logo; these need not mean anything but simply provide a familiar point of reference.

- A 'style guide' should be created for publishers to follow around implementing discovery using the brand created.

The study makes several suggestions for a potential brand, but the one that has received the most attention is 'eduID'.

The idea of using a branded button for log-in is becoming more and more common. As social networking sites such as Facebook, Twitter and MySpace are used by millions of users on a daily basis, many other resources are taking advantage of these captured markets and allowing users to log-in using their credentials from this site. It is becoming increasingly common to see a blog site allowing you to comment by offering a range of clickable buttons from other networking sites. This is possible for two reasons: strength of brand (each social networking site has a well developed simple button that can be reused) and ubiquity of common standards (SAML, OpenID and OAuth¹⁰ are used in nearly all of these scenarios). The federated approach used by access management federations has achieved the second of these aims with its standard use of SAML, but does not offer the strength of brand that is applied by social networking organizations.

Branding, whilst attractive, is not necessarily the answer to all problems and it is essential that any brand is well developed and makes sense to its target market. Attempts by the commercial market to brand have not always been successful. Facebook has recently announced that it is moving away from its 'Facebook Connect' brand as it adopts the more standard approach to access offered by OAuth¹¹. The OpenID protocol has a strong and attractive brand, but although the technology has been adopted, many sites such as Yahoo that make use of OpenID use their own branding by preference. It is important for the research and education community to consider whether it can create a brand that will work internationally, nationally and locally for all of the stakeholders to the log-in process. Simply speaking, it needs to be implementable, it needs to be achievable, it needs to be affordable and it needs to be usable.

In addition to branding, the UK federation has been busily working on improving its own processes. Many publishers and other service providers make use of the vanilla UK federation WAYF, and a new version of this will shortly be

released which uses predictive typing approaches to shorten the drop-down list to a few best suggestions when a user starts typing. It will also offer improved accessibility features based on advice from interface design experts.

For publishers that prefer to develop their own WAYF processes, the Shibboleth software has been developed to improve the code and the GUI for WAYF design, including the features described above. This will make it easier for publishers to integrate the WAYF with their own interfaces whilst improving consistency across different platforms.

Conclusion

The developments described above will make small but significant improvements to the user experience of federated access management, but a larger solution is required. JISC is currently funding consultants to prepare a full business case for the eduID concept, but buy-in from all stakeholders will be essential for it to work. With this in mind we have to continue to ask:

'Would you eduID?'

References

1. UK Access Management Federation for Education and Research:
<http://www.ukfederation.org.uk> (accessed 04 May 2010).
2. SAML:
http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=security (accessed 04 May 2010).
3. Shibboleth:
<http://shibboleth.internet2.edu/> (accessed 04 May 2010).
4. OpenAthens:
<http://www.athensams.net/products-services/OpenAthens> (accessed 04 May 2010).
5. Guanxi:
<http://www.guanxi.uhi.ac.uk/index.php/Guanxi> (accessed 04 May 2010).
6. OpenID:
<http://openid.net/> (accessed 04 May 2010).
7. SimpleSAMLphp:
<http://rnd.feide.no/simplesamlphp/> (accessed 04 May 2010).

8. Atypon SAML SP:
<http://www.atypon.com/> (accessed 04 May 2010).
9. Publisher Interface Study:
http://www.jisc-collections.ac.uk/media/documents/jisc_collections/study-v1.0.pdf
(accessed 04 May 2010)
10. OAuth:
<http://oauth.net/> (accessed 04 May 2010).
11. 'Facebook nixing Facebook Connect branding':
http://news.cnet.com/8301-13577_3-20003075-36.html (accessed 04 May 2010).

About JISC: JISC inspires UK colleges and universities in the innovative use of digital technologies, helping to maintain the UK's position as a global leader in education. JISC provides: a world-class network, access to electronic resources, new environments for learning, teaching and research, guidance on institutional change and advisory and consultancy services.

Article © Nicole Harris

■ Nicole Harris
Services Manager, JISC Executive
Brettenham House, 5 Lancaster Place
London WC2E 7EN, UK
E-mail: n.harris@jisc.ac.uk
Tel: +44 (0)20 3006 6035

To view the original copy of this article, published in *Serials*, click here:

<http://serials.uksg.org/openurl.asp?genre=article&issn=0953-0460&volume=23&issue=2&spage=159>

The DOI for this article is 10.1629/23159. Click here to access via DOI:

<http://dx.doi.org/10.1629/23159>

For a link to the full table of contents for the issue of *Serials* in which this article first appeared, click here:

<http://serials.uksg.org/openurl.asp?genre=issue&issn=0953-0460&volume=23&issue=2>