Implementing Shibboleth Open Source Access Management Software: the DBS Library Experience

David Hughes
Systems Librarian
Dublin Business School
The Pervasiveness of IT systems in HE (and elsewhere)
Access Control

Directory Service for Microsoft Windows based networks
Authentication & authorisation of users
Uses **Lightweight Directory Access Protocol (LDAP)**
Lightweight Directory Access Protocol

Vendor neutral
Industry Standard
Allows sharing of user information

Dublin Business School – Internal IT

Active Directory
Moodle (Virtual Learning Environment)
PaperCut (Print Management System)
College PC login
Email @mydbs.ie
DBS Library – External Services

Koha (Library Management System)
Dawsonera (eBook platform)
Electronic Resources
EBSCO Discovery System
LibCal (Room Booking)
DBS Library Passwords I Have Known

Vendor generated
PIN
Active Directory
Date of Birth
FirstnameYearofBirth
User generated
Too! Many! Passwords!
"We call this one the 'Password Manager.' The vest is made of Post-It notes."

They say an elephant never forgets, but that was before we had so many passwords, user names and PIN numbers!
Incidentally…

Don’t and Do

Don’t reuse passwords
Do consider using a password manager

LastPass
KeePassX

Alternatively

https://xkcd.com/936/
Shibboleth: Simplification/Bridging the Gap
What is Shibboleth?

http://www.merriam-webster.com/dictionary/shibboleth
Origins

http://www.thebricktestament.com/judges/42000_ephraimites_killed/jg12_01.html
Yeah, but what’s Shibboleth?

What’s Shibboleth?

Shibboleth is a standards based, open source software package for web single sign-on across or within organizational boundaries. It allows sites to make informed authorization decisions for individual access of protected online resources in a privacy-preserving manner.

The Shibboleth software implements widely used federated identity standards, principally the OASIS Security Assertion Markup Language (SAML), to provide a federated single sign-on and attribute exchange framework. A user authenticates with his or her organizational credentials, and the organization (or identity provider) passes the minimal identity information necessary to the service provider to enable an authorization decision. Shibboleth also provides extended privacy functionality allowing a user and their home site to control the attributes released to each application.

http://shibboleth.net/about/
Shibboleth

Open Source Software
Middleware
XML-based (Security Assertion Markup Language)
Single sign on inside or outside of organisations
One login, one password
Open Source in DBS Library

- Koha
- Zotero
- DSpace
- Omeka
- LORLS
Middleware

Sits between operating system and applications
Inside
Inside and Outside
Inside the Sausage Factory (1)

You'll need to configure your IdP to consume metadata from our registry at

https://edugate.heanet.ie/hr3/signedmetadata/provider/aHR0cHM6Ly93ZWJhdxRoLmRicy5pZS9pZHAvc2hpYmJvbGV0aA~~/metadata.xml

This feed can be validated with the certificate at https://edugate.heanet.ie/metadata-signer-2012.crt
This is handled in the relying-party.xml.

I recommend you also use our Registry to control the release of attributes, this provides a webpage alternative to hand-editing your XML attribute policy document.
If you avail of this option you will need to configure your IdP to consume an AttributeFilter from

https://edugate.heanet.ie/hr3/arp/format3exp/aHR0cHM6Ly93ZWJhdxRoLmRicy5pZS9pZHAvc2hpYmJvbGV0aA~~/arp.xml

This is handled in service.xml file, here is sample stanza (for Shibboleth V3.x)

    <bean id="FileBackedEduGateAttributeFilter"
        class="net.shibboleth.ext.spring.resource.FileBackedHTTPResource"
        c:client-ref="shibboleth.FileCachingHttpGetClient"
        c:url="https://edugate.heanet.ie/hr3/arp/format3exp/aHR0cHM6Ly93ZWJhdxRoLmRicy5pZS9pZHAvc2hpYmJvbGV0aA~~/arp.xml"
        c:backingFile="%{idp.home}/conf/attribute-filter-edugate.xml"/>

Once you have configured the metadata above, you can test accessing https://edugate.heanet.ie/Whocami with your DBS credentials.
Inside the Sausage Factory (2)
How does it work?

Providers

Identity Providers (IdP) (the library/institution)
Supply user information ("attributes") from LDAP directory

Service Providers (SP) ([the] resource [vendor])
Take user information, assess it and give access to resources
Attributes & ID

- **eduScopedAffiliation**: staff, student (member@dbs.ie)
- **eduPersonPrincipalName**: name
- **eduPersonTargetedID**: college ID number
- **Entity ID/IdP**: Shibboleth server (https://webauth.dbs.ie/idp/)
Shibboleth Usage (1)

Join a Federation

UK (JANET)  Ireland (HEANET)
Shibboleth Usage (2)

Identity/Service Providers join Federations
No membership, no IdP access

But 
eduGAIN

International interfederation service interconnecting national federations
Shibboleth Usage (3)

Alternatively

Bespoke configuration using Security Assertion Markup Language in-house or via third party managed or hosted Identity Provider service.

Will be expensive!
Advantages

Single Sign-On for all campus services
Open Source - free*

Benefits of Federation Membership
Disadvantages

Complex

Requires a lot of heavy lifting by your IT department

Bespoke configuration costs time and money
DBS Library Resource Access Management

The Past (1)

<table>
<thead>
<tr>
<th>RESOURCE</th>
<th>WEB ADDRESS</th>
<th>GLOBAL ACCESS</th>
<th>IP</th>
</tr>
</thead>
<tbody>
<tr>
<td>Emerald</td>
<td><a href="http://www.emeraldinsight.com">http://www.emeraldinsight.com</a></td>
<td>DBS</td>
<td>548169</td>
</tr>
<tr>
<td>FTAF</td>
<td><a href="http://web5g.silverplatter.com/webpers.dbListContent.ws">http://web5g.silverplatter.com/webpers.dbListContent.ws</a></td>
<td>dubar</td>
<td>artlib</td>
</tr>
<tr>
<td>InfoTrac</td>
<td><a href="http://inforac.london.galegroup.com/web.dublin">http://inforac.london.galegroup.com/web.dublin</a></td>
<td>snowdrop</td>
<td></td>
</tr>
<tr>
<td>PayArticles</td>
<td><a href="http://gateway.evid.com">http://gateway.evid.com</a></td>
<td>dubar</td>
<td>artlib</td>
</tr>
<tr>
<td>PayInfo</td>
<td><a href="http://web5g.silverplatter.com/webpers.dbListContent.ws">http://web5g.silverplatter.com/webpers.dbListContent.ws</a></td>
<td>dubar</td>
<td>artlib</td>
</tr>
<tr>
<td>WARC</td>
<td><a href="http://www.warc.com">http://www.warc.com</a></td>
<td>WARC1103</td>
<td>13dub2</td>
</tr>
<tr>
<td>Prerequest</td>
<td><a href="http://prerequestuni.com/login">http://prerequestuni.com/login</a></td>
<td>39MNFT6C86</td>
<td>welcome</td>
</tr>
</tbody>
</table>
Library Resource Management at DBS

- The Past (2)
Why Shibboleth?

Open Athens too expensive
Not all resources available through Athens
Account management
  forgotten username
  forgotten password
  account activation
  account expiry
TOO! MANY! PASSWORDS!
Futureproofing?
Re: OpenAthens account - action required

Hello David I forgot my user id for my Athens login

Regards

On 22 Sep 2014 15:43, “Dublin Business School” <athens-noreply@eduserv.org.uk> wrote:

The following OpenAthens account has been created/modified for you.

Username: dbs

The following link should be used to activate your account:
https://auth.athensams.net/activation.php?username=dbs10161053&activation_code=R5Q25SDGiA

If you cannot follow the link, please copy and paste it into your browser. At busy times it may be a few minutes before this link will work.

If you have any queries about your account please contact your OpenAthens administrator:

David Hughes
Organisation: Dublin Business School
Email: david.hughes@dbs.ie

Before you use this account it is important that you read and understand the Terms and Conditions of Use. See:
http://www.eduserv.org.uk/Legal/OpenAthens
Shibboleth at DBS

The distant past - Joined Edugate
September 2015 - Initial discussions with IT
June 2016 - Shibboleth server
July 2016 New room booking system (LibCal) acquired.
Connected to DBS Shibboleth installation
August 2016 – Initial contact with Vendors
Hi,

We have been using Open Athens to manage access to our electronic resources, including JSTOR. However we are in the process of switching to Shibboleth/SSO to manage access. We’re part of Edugate, the Irish access management federation, but I’m wondering what details you need from us to allow us to switch to Shibboleth authentication, thanks.

Kind regards,

David Hughes

Systems Librarian
Dublin Business School
13-14 Aungier St.
Dublin 2
Ireland

00 353 1 417 8744

david.hughes@dbs.ie
http://library.dbs.ie
Shibboleth at DBS

RE: [CASE:6140736] Shibboleth authentication

ITHAKA Technical Support <techsupport@ithaka.org> 04/08/2016

to me

Thanks David,

We are not currently members of the Edugate Federation, but if you are inter federation enabled and can use eduGAIN, all we would need is your IDP to make the transition, whenever you are ready.

Best,

[Redacted]
Associate Director, Support Services
ITHAKA

ITHAKA is a not-for-profit organization that helps the academic community use digital technologies to preserve the scholarly record and to advance research and teaching in sustainable ways. ITHAKA provides three innovative services that benefit the academic community: JSTOR, Portico, and Ithaka S R.
Shibboleth at DBS

September 2016  Join eduGAIN
DBS Resources commence Shibboleth Authentication
January 2017  Start switching off Open Athens access
February 2017  Open Athens subscription expires.
Go live with Shibboleth for resource access
June 2017  Koha LMS switches to Shibboleth
Why did it take so long?
Conclusions

Me at the start of the project(s)

Me at the end of the project(s)
Shibboleth Advantages redux

Saves money
Open source software
**Single sign on for all college logins**
Access management much easier
Well positioned for the future
Shibboleth Disadvantages redux

Library: Less control over resource access
Too reliant on IT department
    Eggs in one basket
Not all resources Shibboleth compliant (yet!)
Constraints on future resource acquisition?
The Future

Raptor

Non-Shibboleth compliant resources

EZProxy?
If I Could Do It All Over Again…

Do you really want to do this?
Be very very very nice to your IT department
Don’t assume your vendors (or their technical support) will be especially helpful
Give yourself lots of time for the project (nb Parkinson’s Law)
Prepare your users well in advance
No other big projects at the same time
Be patient: you’ll get there in the end
A note about privacy (1)

EU General Data Protection Regulation

new rules for gathering, storing, and processing the personal data of users: companies must obtain users’ consent, and inform them about what data is being transferred and why

Compliance by May 2018

http://www.eugdpr.org/

‘Getting Ready for the GDPR’ Guide
A note about privacy (2)

DBS Active Directory (currently) does not store much user information

  student number

  Email address (@mydbs.ie)
You are about to access the service: 
**Dawson Books Ltd** of Dawson Books Limited

[Additional information about the service](#)

---

**Dublin Business School**
excellence through learning

---

### Information to be Provided to Service

**eduPersonScopedAffiliation**

- **member@mydbs.ie**

---

The information above would be shared with the service if you proceed. Do you agree to release this information to the service every time you access it?

---

**Select an information release consent duration:**

- [ ] Ask me again at next login
  - [ ] I agree to send my information this time.

- [x] Ask me again if information to be provided to this service changes
  - [ ] I agree that the same information will be sent automatically to this service in the future.

- [ ] Do not ask me again
  - [ ] I agree that **all** of my information will be released to **any** service.

---

This setting can be revoked at any time with the checkbox on the login page.

---

[Reject](#)  [Accept](#)
The End

ANY QUESTIONS?