Title
Integrating Multiple Platforms with OpenID Connect, A Shared Authentication Service

Permalink
https://escholarship.org/uc/item/37t0658s

Author
Pottinger, Hardy

Publication Date
2022-06-08

Supplemental Material
https://escholarship.org/uc/item/37t0658s#supplemental

Copyright Information
This work is made available under the terms of a Creative Commons Attribution-ShareAlike License, available at https://creativecommons.org/licenses/by-sa/4.0/
integrating multiple platforms with
OpenID Connect,
a shared authentication service

hardy.pottinger@ucop.edu (CDL)
Next Generation Library Publishing (NGLP)

Partners: Educopia, California Digital Library (CDL), Strategies for Open Science (Stratos), Longleaf Services, Janeway, Confederation of Open Access Repositories (COAR)

- Improve publishing pathways
- Strengthen, integrate, scale-up scholarly publishing infrastructure
- Develop interoperable publishing tools and workflows
- Create community hosting models
- Align with academic values

generously funded by Arcadia

http://nglp2022.org/
NGLP: Technical Overview
Users hate passwords

Password Fatigue

- Too many to remember
- Retyping after every mistake
- Complex requirements
- Update requirements
- Two-factor adds more complexity

What is Password Fatigue and How Can You Overcome it

Survey Finds People Hate Passwords, Go Figure
Supporting people who hate passwords is hard work

Two surveys, in 2000 by Gartner Group, in 2011 by the Ponemon Institute:

- in the year 2000, 30% of helpdesk calls were password related
- each password reset cost the average company about $32
- on average, a user would need four password resets per year
- in 2000, an organization of 3,000 users would have spent $384,000 per year on password resets alone!
- That figure would be much higher in 2011

A Business Case for Single Sign On
Combine/integrate more than one system, it gets worse

- Usability suffers
- Accessibility suffers
- Your helpdesk load increases exponentially

Single Sign-On (SSO) deals with this challenge
Single Sign-On (SSO) Technologies

So many options ([Wikipedia lists 30 implementations](https://en.wikipedia.org/wiki/Single_sign-on#Implementations))

- Shibboleth (SAML)
- Active Directory
- OpenID Connect (OAuth)
1. The RP (Client) sends a request to the OpenID Provider (OP).
2. The OP authenticates the End-User and obtains authorization.
3. The OP responds with an ID Token and usually an Access Token.
4. The RP can send a request with the Access Token to the UserInfo Endpoint.
5. The UserInfo Endpoint returns Claims about the End-User.

Uses OpenID Connect-specific terms, but the concepts are the same for SAML/Shibboleth.
OpenID Connect (OIDC)

- interoperable authentication protocol
- based on OAuth 2.0
- uses REST/JSON message flows
- design goal of “making simple things simple and complicated things possible”.
- easy for developers to integrate

https://openid.net/connect/faq/
Who uses OIDC, anyway?

- Google
- Gakunin (Japanese Universities Network)
- Microsoft (yes, Azure)
- Ping Identity
- Nikkei Newspaper
- Tokyu Corporation
- mixi
- Yahoo! Japan
- Softbank
- Deutsche Telecom
- AOL
- Salesforce
- NGLP
OIDC Options

Self-Hosted

https://www.keycloak.org/

Many commercial offerings

https://openid.net/developers/certified/#OPServices

Hosted

AWS Cognito

Microsoft Azure Active Directory
Existing Integrations of OIDC

- DSpace-CRIS 7 2021.02.00 October, 27th
- DSpace 7.1
- Janeway 1.4.2
  [https://www.nature.com/articles/s41597-020-0429-3](https://www.nature.com/articles/s41597-020-0429-3)
- Possibly Avalon (Samvera)
- [https://openid.net/developers/certified/](https://openid.net/developers/certified/)
Porting DSpace-CRIS OIDC authentication to DSpace

Original work by Luca Giamminonni (4Science)

- Reworking of the existing Shibboleth plugin for OIDC
- Required a bit of detangling from additional DSpace-CRIS functionality
- Thanks Luca for pointing out the parts we didn’t need to port
- Worked immediately in the CDL DSpace 7 pilot instance
- Documenting how to test the contribution was challenging
- Thanks Tim Donohue for your patience and perseverance
DSpace OIDC Authentication Plugin Demo

https://dspace-pilot.escholarship.org/
Testing OIDC authentication

https://www.phantauth.net/

- OpenID Connect Provider
- Random User Generator
- Lots of documentation and examples
- Free!

https://github.com/DSpace/DSpace/pull/8088 (DSpace 7 testing process)
OIDC in NGLP

OIDC is up and running at our NGLP pilot sites

https://www.nglp2022.org/pilots
Ask me a question. Please.

Attribution:

lock picking meme

man in gray crew neck shirt covering his face with his hand

man in gray crew neck shirt smiling

Give me a shout:

hardy.pottinger@ucop.edu

@HardyPottinger

@hardyoyo@code4lib.social