Federated authentication for library resources: can it be trusted?

UKSG webinar – Wednesday 14th July 2021

Lee Houghton, Heather Flanagan, Jos Westerbeke, Kelechi Okere

Access via IP recognition

Campus areas enclosed in a defined network of IP addresses

Access automatically granted – no usernames or passwords required

Certain degree of privacy preserved – 3rd party would not know who was signed in to the campus PC

Proxy services

IP access outside the campus bubble is not available

Proxy services deal with the off campus access dilemma

Single IP address is passed to the e-resource provider, preserving a degree of privacy

Federated authentication

Expectations and needs of library users has changed

Users have multiple starting points: browser bookmarks, Google or Google Scholar (or both)

Federated authentication offers direct access using institutional credentials

Communication channel established between e-resource ('service provider') and academic institution ('identity provider')

Identity federation (UKAMF) manage this communication at scale

SeamlessAccess

Federated authentication configured and implemented differently by different service providers, leading to bad user experience

SeamlessAccess core aim is to make it easy for users to move from one service provider to another

User doesn't need to search for their institution – 'where they are from' is saved in their local browser

SeamlessAccess

SeamlessAccess

SeamlessAccess

Wider adoption of SAML

Large increases in use of federated authentication on platforms that have implemented SeamlessAccess

Encourage more e-resources and institutions to use SAML

Best practice for configuration and implementation needed to ensure good user experience and preserve privacy

Core FIM4L principles:

1. Federated authentication is a viable alternative to IP based access with a strong set of benefits for libraries and publishers

2. Correct configuration is key to the successful operation of a Single Sign-On connection

3. User privacy should be always be protected by all parties involved

SAML and user privacy

Library is in control of privacy levels

IdP can be configured to release either a transient or a persistent alphanumeric identifier

Service providers can ask for additional attributes but personal information (name, email) should always be optional for the user

Useful links

FIM4L recommendations: https://www.fim4l.org/?page_id=257

SeamlessAccess: https://seamlessaccess.org/

REFEDS (the Research and Education FEDerations group):
https://refeds.org/

UK Access Management Federation for Education and Research:
https://www.ukfederation.org.uk/