Overview of ORCID use by Proxy IdP

ORCID IoLR Integration Draft

Summary

Most academic researchers can use their institution's own Identity Provider (IdP) to authenticate with online resources. However, a relatively small number of researchers do not have access to an IdP, or require access to research services that do not allow access using their organisation's IdP.

Proxy IdPs can act as an IdP for these users by authenticating people using accounts they already have elsewhere - such as Google, Facebook, or ORCID.

This document outlines how and why ORCID can be useful as an authentication source for a proxy IdP that acts as an "IdP of Last Resort" (IoLR) for users with no institutional IdP.

Terminology

IdP: An authentication service, such as a university's Shibboleth login service. Usually authenticates an institution's users using a database of members of the organisation.

Proxy IdP: An IdP that uses external sources for authentication, such as other IdPs or websites. It is *not* the same sort of proxy as a web proxy used to access the Internet, or an access control proxy like EZProxy.

IdP of Last Resort: It is usually best for academic users to log in to federated websites using an IdP from their home institution (a university, college, or school). When this is not possible users may use accounts at a third-party IdP, or a special IdP managed by the organisation they need to access.

Use Cases

Research collaboration with Chinese researchers

Technical Overview

Configuration of The Proxy IdP

(Focus on needing to be an OpenID Connect client OR OAuth)

Official Documentation

Configuration of the User Interface

(Focus on WAYF/disco design)

Configuration of ORCID

Potential Issues

User Experience (Discovery UI)

Load

Support

Examples

LIGO/CILogin

MWA

Géant EduTEAMS

FAQ

Why use ORCID? Why not use Google or Facebook?

Social media services tend to be weak for privacy and security and are often banned or restricted in some countries.

Researchers may not want their work and personal personas to overlap.

Why not use ORCID directly?

ORCID is not a SAML IdP and is not designed to be used as a general purpose IdP.

Could ORCID handle the load from being used for authentication?

In order to provide Single Sign On (SSO) the proxy IdP would probably only need to direct users to log on at ORCID once per session. After successfully authenticating with ORCID, users of the proxy IdP could then log in to many other services without any further calls to ORCID until the session expires, typically after six hours. A proxy IdP would therefore put less load on ORCID than if the various resources were authenticating with ORCID directly.

Despite this the proxy would still be sending additional requests to ORCID, and only realistic load testing would indicate if the additional traffic is significant.

ORCID does not support SAML

The proxy IdP uses SAML to the resource the user is trying to access, but uses a protocol supported by ORCID to authenticate the user (instead of using its own LDAP directory and passwords).

(Diagram)

Who would run and manage the proxy IdP?

Are passwords and other credentials shared or exposed?

No. The user's browser is redirected by the proxy to ORCID, authenticates with ORCID, and then returns to the proxy before being redirected to the service the user wishes to access. No passwords would be shared, and no ORCID credentials would be entered into the proxy.