OpenID Connect (OIDC) Provider

Introduction

Finna has support for OpenID Connect that allows third parties to request user authorization while giving the user control over the process. The user can see what information is being requested and grant or deny the request case by case.

See OpenID Connect Primer for an introduction into OIDC and how the process works.

For an example of a service using OpenID Connect with Finna, see the Prenax e-journal service of PIKI Libraries.

Instructions and Guidelines

- Please contact finna-posti@helsinki.fi first.
- The service is only available on agreement.
- Make sure to request only the bare minimum of information you need for required functionality. For instance if you need to know user's age, use the age scope instead of birthdate.
- Please note that Finna consists of different instances for specific audiences. To limit the eligible user accounts, use the OIDC provider of a specific instance instead of finna.fi.
- Server's keys are available at /OAuth2/jwks (e.g. https://www.finna.fi/OAuth2/jwks)
- Authorization endpoint is /OAuth2/Authorize
- Token endpoint is /OAuth2/Token
- User information endpoint is /OAuth2/UserInfo

Required Information

To use OIDC with Finna, we will need the following information about the client:

Entry	Description	Examples
Identifier	Something that properly identifies the client instance. If the service has a single URL for all audiences, it could be just the service name. Otherwise it should include the target audience. Could also be just a random string.	coolservice coolservice_libraryname Xn9fFr6IKJ6MW4Muza6MeS6zf0Wv2XnxlwLw9yUApbDNTAt9PfBK
Redirect URI	A URL of the client where the user's browser is redirected after authorization	https://coolservice/oauth2/result
PKCE support	Whether the client supports PKCE. PKCE is mandatory for non-confidential clients (e.g. in-browser apps)	yes/no
Confidentiality	Can the client keep its secrets (runs on a server, is confidential) or not (runs in a browser, is not confidential)	yes/no
Shared Secret	A password shared between Finna and the client. This needs to be communicated securely.	ieUmLbwlya1kJLEZgc.ePNTEXuRlhWSgRVS03eyFQUawlzAQg22

Supported functionality

Finna supports the authorization code flow.

The following scopes are available in addition to the standard scopes *openid*, *profile*, *email*, *address* and *phone* defined by the OIDC specification:

Scope	Description
id	User's unique identifier in Finna
name	User's name (full name, first name, last name)
age	User's age calculated from birthdate (see below)
birthdate	User's birthdate returned by a library for a library card
locale	User's current language
block_status	Whether the user has blocks (e.g. a borrowing block) placed for their library card. Possible values are true (blocks set), false (no blocks) or null (status unknown)

library_user_id	A unique one-way hash of user's identifier in the library system
library_card	User's library card number
auth_method	User's primary authentication method

Further Information

- Details on the implementation can be found in the VuFind wiki.