Integrate OpenAthens Keystone

Our service desk will be happy to help at any stage.

Preparation

- Make sure you can access the publisher dashboard at sp.openathens.net.
- Create a test account at admin.openathens.net (same credentials as the publisher dashboard)
    - See OpenAthens test accounts for more advanced test account options

Install an OpenID Connect plug-in or framework

1. If you do not already have an OIDC plug-in or framework installed, find one for your platform that has agreeable documentation and install it. This must support "OpenID Connect" specifically, rather just OpenID (which is older and will not work with OpenAthens).
2. Configure your site to use the plug-in or framework and add the option to your login page alongside any other login methods you have. For help with that you will need to consult the documentation of your chosen plug-in and platform. See also: OpenID Connect examples

Configure the basic application in the OpenAthens publisher dashboard

1. Access the publisher dashboard at https://sp.openathens.net
2. Add a new application, choosing OpenID Connect from the options
3. Fill in the form
    a. All the fields on the first page can be changed later if necessary, but must be valid to proceed.
    b. Select a new connection unless you are migrating from one OIDC app to another
4. Click the create application button
5. This will create the record and display the details you need to configure your OIDC plugin

For a more detailed view of these steps, see: Adding a new OIDC application to the publisher dashboard step by step

Configure your OpenID Connect plugin or framework for OpenAthens

1. Access the configuration of your plugin or framework and update the settings to connect to OpenAthens.
2. (a) and (b) below are always needed. Some or all all of the others *may* need to be specified. There can also be some small variation in terms:
    a. Client ID & Client secret or key - copy both from the dashboard > application > configuration tab
    b. Provider URI - `https://connect.openathens.net`
    c. Login or Authorisation endpoint - `https://connect.openathens.net/oidc/auth`
    d. Token (validation) endpoint - `https://connect.openathens.net/oidc/token`
    e. User Info endpoint - `https://connect.openathens.net/oidc/userinfo`
    f. JWKS / Key URI - `https://connect.openathens.net/oidc/jwks`
    g. Identity key / claim / attribute - this should usually be set as 'sub' (as in subject)
3. Your plug-in or framework will probably support automatic configuration in the background, but if you need to specify the address manually (or check any of the content) it is https://connect.openathens.net/.well-known/openid-configuration (the dot before well-known is necessary)

Test

You're not finished, but at this point you can start the 'works at all' tests as invoking your OIDC login will send you to your own OpenAthens login point where you can sign in with a test account. If it's working you should receive a few claims.

The most likely problem to come up at this stage is an invalid redirect URL error, fixed by updating the return URL in the publisher dashboard to match the address of the error, less any parameters (Application > Configuration tab).

Next

Once you have it working in this basic way, it's time to look at the integration with your existing authorisation flow and how to deal with the data that your customers in the federation will be sending. This is covered in the continued integration of Keystone page.