Best practices

This section covers best practice when implementing support for federated access in general and specifically in the OpenAthens Federation.

How users arrive at your website

There are two scenarios that need to be considered:

- When a user arrives at your site from anywhere (such as from a Google search).
- When a user arrives at your site from their organisation's portal.

In both scenarios the end result should be the same: that the user has been authenticated by their Identity Provider, the Service Provider has confirmed their authorisation and a local session has been set up on the user's behalf.

For the first scenario you will need to implement a discovery service (sometimes called a WAYF for Where Are You From) in which users will be able to choose their organisation from a list so you can send them to their institutional log on page with a SAML request. This list will ideally be accessed via a type-ahead rather than a drop down as there can literally be thousands of IdPs that appear. You can write your own, but using a central discovery service such as OpenAthens Wayfinder is encouraged for consistency (See: Discovery)

For the second scenario where users follow a curated link, wayfless URLs should be supported if possible - i.e. links that include the IdPs entityID and avoid additional discovery; e.g. https://sp.yourdomain.com?entity=<IdP_entityID>&target=<targetURL>. This kind of URL is incredibly popular with IdPs who wish to simplify user access. These links should use federation entityIDs rather than your own customer IDs for compatibility with other systems.

Where users follow a login link on your site they should, wherever possible, end up at the same page - e.g. if the login link is on an article abstract, the user should end up back at that abstract with whatever additional content now available.

Terminology

There has been much discussion on what terminology should be used on login pages; a common theme is that users should not see technical terms such as Shibboleth (or OpenAthens) on login pages. We endorse the approach summarised by REFEDS, the TERENA group which looks at the needs of existing and emerging e-identity federations operating in the field of education and research. For examples and more detailed ideas about industry best practice on contributing to creating a familiar login experience for users, see the REFEDS Discovery Guide which distils the section 4.4 Recommendations to Service Providers of the ESPReSSO: Establishing Suggested Practices Regarding Single Sign-On project report. The most important parts can be briefly summarised as:

- The 'login' button or link should be in the top right of the page
- In the login dialogue, use a term such as 'Institutional login' to describe this kind of access rather than naming a technology
- If you are in multiple federations, the user signing in shouldn't need to know about it

This does not mean you cannot accommodate requests from your customers for special treatment.

Authorisation

A common method to authorise users is based on the organisation they are from, and this can be implemented by making use of the organisation identifier (scope). You should not use entityID for authorisation as it prevents you providing different levels of subscription across large organisations or consortia. It is also possible to perform more granular authorisations based on attributes such as role or entitlements.

Authorisation error messages

When a user is not authorised for access, an error message should tell them why - e.g. "your organisation does not have access to this section" is better than "error code 4 ref: o8ysiuyrt88str".

Attributes

The exact attributes passed when an end-user accesses your resource depends on how the Identity Provider is configured however there are some standard attributes you can expect to receive.

Federations normally provide recommendations about what attributes should be passed or used for which purpose and you can expect IdPs in that federation to be able to pass them however they are likely to default to passing only the barest minimum unless you tell them which attributes you need. For details about standard and extended attributes in the OpenAthens federation, see: Standard attributes in the OpenAthens federation

You may want to use some items of personal end-user data to enhance their experience, e.g. to avoid a separate registration process. The GÉANT Data Protection Code of Conduct for Service Providers in EU/EEA attempts to define behavioural rules for Service Providers which want to receive user attributes. It is our experience though that identity providers are very reluctant to release personal information, even without GDPR and similar legislation, so you should not expect it and must not require it.

Deep linking

Deep linking (or article level linking) via authenticated links should be supported wherever possible as this is highly desirable to your customers. Your implementation should allow a target page variable to be passed to the authentication process for the user to be directed to after authorisation and any customer identifiers included in these access URLs should be those used by the federation to allow links to be tokenised in a consistent way (e.g. use the subscribers' federation entityIDs rather than your own subscriber number).

Unique identifiers

In order to ensure uniqueness of records, any data which you hold about users needs to be associated with a unique user identifier, ideally a pseudonymous one. The OpenAthens Federation uses the eduPersonTargetedID attribute which is usually suitable.

Logging out

Where a logout function exists, it should be clear to the end-user that they have been logged out of your service.

If you wish to offer the user the option to also logout from their identity provider when they log out of your site, it must be separate from the logout of your site – i.e. a user choice. See: Logout function

Expired Sessions

When sessions expire, you should wherever possible allow them to restart their session at the same page.