Notes from meeting held in Cardiff, November 2009

Attendees

- Chad La Joie
- Rhys Smith
- Rod Widdowson
- Ian Young

Implementation Details

Service Provider Front Page

All space on the front page of most providers is considered to be very valuable. Today, most providers have one of three different mechanisms for starting the login process:

just-in-time authentication where the provider allows the user to browse around the site until they try to access a restricted resource at which point the authentication process is automatically started:

- a “login” link/button usually located in the upper right of the window;
- a login panel, usually located in the left margin of the page, containing a username/password entry form;
- For those service providers that rely solely on federated authentication a “Login” link, located as the upper-right-most corner of the page is suggested. The link would lead to the IdP Selection Page described below.

No recommendations are currently given for starting the IdP selection process, for service providers which offer multiple modes of authentications.

IdP Selection Page

The IdP selection page will be a box with the top half containing a list of “preferred” identity providers identified by their logo and textual name. The preferred identity providers may either be set explicitly by the page deployer or be populated from past selections made by users on the visiting computer. At least one space must always be available for such a user-selected organization. The total number of icons should never exceed three or four. Clicking on the link or logo sends the user on to the next login step.

Below that will be a search-as-you-type entry field where a user may enter in the name of their organization. The user may enter either parts of their organization?s name or its domain name. This text area will have the focus once the page loads and the button to progress to the next step has been labeled “continue”. The ability to remember the selection for differing periods of time has been removed. Few users in usability test understood what it meant.

Finally there are two links at the bottom of the box. The first link “Show me a list of all organizations” will provide a listing of all known identity providers from which a user may choose one. This will assist those that unsure what to type in the box and may also assist certain movement impaired individuals. The second link will open a new page describing what this login process is and what to expect as the user goes through it.

The recommendation would be to deploy this page directly on the service provider with the selection box surrounded by the SP?s native look and feel. The data for the page would, ideally come from an endpoint on the service provider itself in order to decrease reliance on external services which might be down or slow to respond. Until such time as service providers with the ability to serve up the necessary information are deployed centralized discovery services should provide the necessary information. Finally, if this is not available, the SP should redirect to the external discovery service which should provide an IdP selection page as described here.

The rendering of the discovery data, whether from the SP or a centralized source, in to the discovery panel would be handled by a set of HTML/CSS /Javascript. Deploying it would require filling in a property file and put the files out on the service provider?s web server.

Identity Provider Login Page

Carrying forward nested box UI the login page for the IdP should contain two panels inside the primary box. On the left would be the authentication panel (mostly like a username/password form). On the right be a service provider identifier panel that contained the logo, name, and description of the service provider. This provides continuity to the process so that the user is more likely to understand that they are still performing the actions necessary for the identified SP.

Like the identity provider selection page, the nested boxes would be on a page which had identity provider specific branding around it.

Attribute Consent Page

Identity providers are strongly encourage to deploy an attribute release consent module like uApprove. Even if consent is not strictly required informing the user what information is to be released is still a good practice. The consent page will look like the login page with the authentication panel replaced by the consent panel.

Future Work

Service Provider Front Page

There are a number of possible alternatives UI elements which could be tested for use on the front page. One option is the use of an Amazon-stye link [Login in from Foo University (Not from Foo University, click here)] after an initial identity provider has been selected. One concern here is that some organizational names are quite long and may lead to poor layouts. It may be possible to use the organization?s domain name in place of its formal name.

Another option would be to create a branded button the identified the “login with federated identity” process. It is felt that creating such a brand that identified the process without being too restrictive (i.e. federation or even sector based) would be very time consuming and so is not a pragmatic option at the moment.

Finally, in order to address sites with multiple modes of authentication a site could, when using an authentication panel on the front page, allow a user to initially select the form of authentication to use. Upon subsequent visits the user would simply be presented with the UI for the local authentication mechanism or the the previously selected identity provider with an option of moving in to the IdP selection process if that was not the one they wanted.

Requisite Metadata Changes

In order to render the necessary information the following additional data would need to be added to an IdP and SP metadata:

- a logo - a link to a logo for the entity. Multiple links, to images of different sizes could be provided. Recommendations on size, or aspect ratio, should be provided;
- Metadata registrars should takes steps that any registered logo properly represents the service;
- localized entity name and description;
- URL to the help page for the entity;
- IP address ranges for the organization - may be used to offer hinting as to which organization a user is trying to select during the IdP selection process.