**DiscoveryService**

**Why Deploy a Discovery Service?**

A discovery service is a solution to the IdPDiscovery problem. Briefly summarized, it seeks to solve the problem facing an SP when a user first approaches it:

"Where can I direct this user to go to acquire the credentials I need to allow them access to the pages they want to visit"?

If the SP knows that only one IdP will ever provide authentication then it can immediately send the user to that IdP. However, an SP will usually be able to handle users authenticated by multiple IdPs and at that point it has no option but to ask the user to select an IdP, which is usually done by a Discovery Service.

Although this solution is deceptively simple it is complicated by several factors:

- Any user interaction associated with this operation will be the first that the user ever sees and hence will define the user's opinion of the SP.
- Even returning users may not be aware of precisely what is being asked of them ("What is a Federation?", "What is an IdP?", "Why do I need to do this?")
- An independent service is not well positioned to provide simple choices because it has to make broad assumptions as to which IdPs might be of interest. This has two potential side effects:
  - It will offer a confusing list of IdPs to the user
  - It can allow a user to select an IdP which cannot provide authentication to the SP.
- SPs are very often members of more than one Federation

These issues can be minimized by associating a discovery service with each SP. Thus deployed the discovery service can:

- Have a similar look and feel to the rest of the SP.
- Provide assistance in selecting the IdP in a way which is targeted at its particular users base.
- Limit those IdPs which the user is asked to chose from to those which the SP is willing to accept authentication from (for commercial, technical or other reasons).

In addition to per-SP discovery services, most federations deploy a discovery service. This serves as the 'back stop' service. It is considered best practice that SPs have a specific discovery service, however those SPs which are only in one Federation can rely on this Federation-deployed discovery service.

**Example**

As an example, consider a commercial SP with contracts with three institutions: Institution A is a member of InCommon, Institution B is a member of the UK federation and Institution C is a member of the SWITCHaai Federation

When a user approaches the SP, they should not be presented with a list of all the IdPs known to all three Federations, as the SP only needs to know which of these three IdPs the user needs to be sent to. The SP can provide guidance to the user in selecting one of these couched in terms that their target audience can understand.

**What does the Discovery Service do?**

In Shibboleth version 1.3, the discovery service takes an AuthnRequest message as input and, as a result of interaction with the user, forwards this message on to the selected IdP.

In Shibboleth version 2.0 the discovery Service can also handle the Discovery Service Protocol

The discovery service can keep track of the IdP that was selected by using the browser cookie specified in the Identity Provider Discovery Profile. However this can only store the fact that an IdP was selected, not whether the user authenticated successfully (in which case the user might wish to change their choice of IdP). Hence, by default the discovery service does not automatically redirect the request to the last selected IdP, instead a list of the most recently selected IdPs is provided as a hint.

The discovery service uses SAML2 metadata to find out about the Entities (SPs and IdPs) that it interacts with. For a per-federation discovery service this is usually the same as metadata which the federation publishes. For an SP-specific discovery service this input metadata would be constrained to only list the relevant SP and IdPs. Once deployed, the discovery service watches the metadata files and will reload them as soon as they are changed.