Discovery Service

InCommon Discovery Service

The *InCommon Discovery Service* is a centralized IdP discovery interface for all InCommon participants. Visit our web site for a brief history of discovery or visit the Discovery Service FAQ for more information about the InCommon Discovery Service.

Software and Metadata Considerations

Configuring Metadata for Discovery

If your SP supports SAML V2.0, and the SP is configured to use the *SAML V2.0 Identity Provider Discovery Protocol*, you **must** configure your SP's metadata to include one or more `<idpdisc:DiscoveryResponse>` elements. If you don't, a request to a properly configured discovery service endpoint (such as the InCommon Discovery Service) will fail.

If you inspect InCommon metadata, you will find extension endpoints such as the following in SP metadata:

<idpdisc:DiscoveryResponse> metadata extension element

```
<idpdisc:DiscoveryResponse index="1"
    xmlns:idpdisc="urn:oasis:names:tc:SAML:profiles:SSO:idp-discovery-protocol"
    Binding="urn:oasis:names:tc:SAML:profiles:SSO:idp-discovery-protocol"
    Location="https://carmenwiki.osu.edu/Shibboleth.sso/Login"/>
```

The namespace and binding attributes attached to the `<idpdisc:DiscoveryResponse>` element are defined in the *SAML V2.0 Identity Provider Discovery Protocol and Profile* specification. The endpoint location is the return address for the SP, that is, where the Discovery Service returns to once the user's preferred IdP has been determined.

Likewise if your SP is configured to issue SAML V2.0 authentication requests, you **must** add one or more SAML V2.0 `<md:AssertionConsumerService>` endpoints to your metadata. (The same is true of SAML V1.1, by the way.) Failure to do so will result in errors when such requests are issued to IdPs, since your metadata will lack sufficient support for the desired protocol.

The Discovery Service and the IdP have similar requirements with respect to metadata. Both components will redirect the browser user back to the SP, but only to a **trusted endpoint** at the SP. Those endpoints **must** be called out in SP metadata, otherwise the protocol is violated and the redirect will not occur.

Configuring your SAML Service Provider Software

In general, configuring your SP software for discovery depends on the protocol(s) it supports. If your SP supports SAML V1.1 only, you **must** configure your SP to use the legacy WAYF protocol, which is based on the proprietary Shibboleth 1.x AuthnRequest protocol. If your SP supports SAML V2.0 only, you **must** configure your SP to use the *SAML V2.0 Identity Provider Discovery Protocol*. In that case, you **must** configure SP metadata as described in the previous section.

Of course, if your SP supports both SAML V1.1 and SAML V2.0, you have a choice, but clearly SAML V2.0 is preferred since it offers a much richer set of deployment options. Note that some SP implementations are sophisticated enough to make a runtime decison based on the supported protocols called out in IdP metadata.

Instructions how to configure the Shibboleth SP for discovery can be found elsewhere in this wiki.