SP Metadata

From RavenWiki

Introduction

Shibboleth IdPs and SPs can publish 'Metadata' about themselves in XML (SAML v1.1 (http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml1x-metadata-os.pdf) , SAML v2 (http://docs.oasis-open.org/security/saml/v2.0/saml-metadata-2.0-os.pdf)). Typically SPs need access to the metadata describing the IdPs that they work with, and vice versa.

For SPs registered with the UCam federation, a copy of their metadata is stored within the Raven IdP - a copy of the Ucam federation metadata file can be accessed at https://shib.raven.cam.ac.uk/ucamfederation-sp-metadata.xml. For SPs in the UK federation their metadata is included in the UK federation metadata file (http://metadata.ukfederation.org.uk/ukfederation-metadata.xml) .

SPs metadata normally associates three things:

- The SP's EntityID
- The URLs of services offered by the SP (in particular the "Assertion Consumer Service" (ACS) URLs to which IdPs can post assertions)
- Certificate(s) describing the cryptographic keys used by the SP

The information in the metadata must match the SP's configuration and may have to be updated after configuration changes. This can be a problem since copies of the metadata are stored elsewhere and so should be avoided wherever possible. A mismatch between metadata and configuration will generally cause things to fail in strange ways, often with unhelpful error messages.

Creating Metadata

The normal configuration of the Internet SP sets up an automatic metadata generator which will generate metadata matching the configuration. You can access it it at:

```
http://<host-name>/Shibboleth.sso/Metadata
```

or, if your site supports https:

```
https://<host-name>/Shibboleth.sso/Metadata
```

The auto-generated metadata is not intended to address every eventuality. It's an XML file and there is nothing to stop you from editing it after generation (assuming you know what you are doing) or even creating it by other means.

The scheme (http vs. https) of the ACS URLs in the generated metadata will match that of the URL used to generate it. That's fine for a http-only website, but for one that supports both http and https this can cause problems when someone accesses the site using a different scheme from that used in the metadata.

The full explanation appears below, but the problem can be avoided in several ways:

- Force all access to the site to be over https. This is probably the best solution since it also provides better security (see SSL, certificates and security with Shibboleth). This can either be done within the web server or the site it is serving, or by the SP using either the ShibRedirectToSSL Apache directive (`ShibRedirectToSSL <portnumber>`) or by setting the 'redirectToSSL (https://wiki.shibboleth.net/confluence/display/SHIB2/NativeSPRequestMapper#NativeSPRequestMapper-Properties) ' attribute of a <RequestMap> (https://wiki.shibboleth.net/confluence/display/SHIB2/NativeSPRequestMap) , <Host> (https://wiki.shibboleth.net/confluence/display/SHIB2/NativeSPRequestMapHost) , <HostRegex> (https://wiki.shibboleth.net/confluence/display/SHIB2/NativeSPRequestMapHostRegex) , <Path> (https://wiki.shibboleth.net/confluence/display/SHIB2/NativeSPRequestMapPath) , <PathRegex> (https://wiki.shibboleth.net/confluence/display/SHIB2/NativeSPRequestMapPathRegex) or <Query> (https://wiki.shibboleth.net/confluence/display/SHIB2/NativeSPRequestMapQuery) element to the https port number within the shibboleth2.xml <RequestMapper> (https://wiki.shibboleth.net/confluence/display/SHIB2/NativeSPRequestMapper) element. Note that you ***can't*** add this property to the <RequestMapper> (https://wiki.shibboleth.net/confluence/display/SHIB2/NativeSPRequestMapper) itself - adding it doesn't casue an error but it doesn't work either. The https port number is commonly 443.
- Set the 'handlerSSL' attribute of the <Sessions> (https://wiki.shibboleth.net/confluence/display/SHIB2/NativeSPSessions) element to "true". This will force all ACS URLs (and other internally-serviced URLs) to use the https scheme but will continue to allow the content of the site to be accessed over http. (Re-)generate the metadata using the https scheme.
- Register both http and https URLs in the SP metadata. This can be most easily achieved by adding https="true" http="true" attributes to the <Handler type="MetadataGenerator"> (https://wiki.shibboleth.net/confluence/display/SHIB2/NativeSPHandler) entry in shibboleth2.xml and then re-generating the Metadata.
- Disable http support completely.
- Disable https support and re-register your SP using just http: ACS URLs.

The full story

SP Metadata includes a list of the ACS URLs (in one or more <md:AssertionConsumerService> elements) to which IdPs are allowed to return information. When an SP makes an authentication request it includes (typically in the 'shire' parameter) the ACS URL to which it wants the results returned on this occasion.

SPs create ACS URLs from information in the shibboleth2.xml file (the 'handlerURL' and 'handlerSSL' attributes of the <Sessions> (https://wiki.shibboleth.net/confluence/display/SHIB2/NativeSPSessions) element and the 'Location' attribute of the relevant <AssertionConsumerService> (https://wiki.shibboleth.net/confluence/display/SHIB2/NativeSPAssertionConsumerService) element), and from the details of the virtual host handling the current request. In the default configuration, the SP uses the scheme (http: or https:) and host name of the virtual host and the values of the 'handlerURL' and 'Location' attributes to construct an ACS URL. In the default configuration, an authentication request using the SAML 1.0 Browser/POST profile triggered by access to

```
http://www.example.cam.ac.uk/secure/
```

would include this as an ACS URL:

```
http://www.example.cam.ac.uk/Shibboleth.sso/SAML/POST
```

A problem occurs when accessing an SP over http whan it also supports https and has registered https assertion consumer service URLs in it's metadata. In this case the ACS URL generated will be for http and these won't match those in the metadata. This causes the IdP to report "Invalid assertion consumer service URL" or "No peer endpoint available to which to send SAML response" and to refuse to process the request. Despite the message being reported by the IdP, it reflects a problem on the SP.

Retrieved from "https://wiki.cam.ac.uk/wiki/raven/index.php?title=SP_Metadata&oldid=2488"

- This page was last modified on 21 June 2012, at 11:48.
- Provided by Computing Service, University of Cambridge