IdP ECP Extension

This plugin has been moved in to the core IdP distribution as of V2.3 and this documentation does **NOT** apply to the built-in version. ECP support is enabled by default in the configuration files that are shipped with V2.3 provided that container or web server authentication is enabled for the profile path of **/idp/profile/SAML2/SOAP/ECP** so that REMOTE_USER is set. More at IdPEnableECP.

IdP ECP Extension

This extension to the Shibboleth 2.x IdP adds some support for ECP. Authentication to the IdP from the enhanced client is limited to Basic Authentication.

See the SAML V2.0 Profiles Specification for details of the ECP profile.

Installation and configuration

Prerequisites

- An installed Shibboleth 2.x IdP
- Basic Authn capability. Usually provided by Apache or Tomcat.

Installation

1. Download the ECP extension.
2. Run '`$mvn install`' to build.
3. Copy the target jar, `shibboleth-idp-ext-ecp-`*`VERSION`*`.jar` to your *idp-distribution*`/lib` directory.
4. Rerun the IdP's install script to build a new war file.

Configuration

`handler.xml`:

1. Add this namespace definition:

```
xmlns:ecp="urn:mace:shibboleth:2.0:idp:ext:ecp:profile-handler"
```

2. Add to the schema location:

```
urn:mace:shibboleth:2.0:idp:ext:ecp:profile-handler classpath:/schema/shibboleth-2.0-idp-ext-ecp-profile-handler.xsd
```

3. Add a profile handler declaration for the ECP SOAP handler

```
 <ProfileHandler xsi:type="ecp:SAML2ECP"
     inboundBinding="urn:oasis:names:tc:SAML:2.0:bindings:SOAP"
     outboundBindingEnumeration="urn:oasis:names:tc:SAML:2.0:bindings:SOAP">
   <RequestPath>/SAML2/SOAP/ECP</RequestPath>
 </ProfileHandler>
```

`relying-party.xml`:

1. Add this namespace definition:

```
 xmlns:ecp="urn:mace:shibboleth:2.0:idp:ext:ecp:relying-party"
```

2. Add to the schema location:

```
 urn:mace:shibboleth:2.0:idp:ext:ecp:relying-party classpath:/schema/shibboleth-2.0-idp-ext-ecp-relying-party.xsd
```

3. Add an ECP profile configuration to the default relying party definition or to each relying party's definition for whom you want to support ECP, e.g.:

```
<ProfileConfiguration xsi:type="ecp:SAML2ECP"
   includeAttributeStatement="true"
   assertionLifetime="300000"
   assertionProxyCount="0"
   signResponses="conditional"
   signAssertions="always"
   encryptAssertions="never"
   encryptNameIds="never"
 />
```

Signing and encryption options may vary with your cilents.

Basic auth

Configure your server to require Basic Auth for the ECP location. For Apache you might use:

```
<Location /idp/profile/SAML2/SOAP/ECP>
  AuthType kerberos
  AuthName "SAML2 ECP"
  require valid-user
</Location>
```

Test

A simple test is provided in the doc directory.

1. Edit the testecp.sh shell script for your installation.
2. Run the the script, from the IdP host or from a remote site.

Metadata

According to the SAML V2.0 Errata an IdP supporting ECP can advertise a binding of:

```
urn:oasis:names:tc:SAML:2.0:bindings:SOAP
```

and an SP can advertise:

```
urn:oasis:names:tc:SAML:2.0:bindings:PAOS
```