InCommon Silver Interop Test Case Zero

Purpose of Test

The purpose of this test was to determine the feasibility of asserting level of assurance via a method other than attribute. The specific implementation was designed to test passing assurance via authentication context handler.

Overview of Functionality

Normally SAML asserts user information via attributes. This method essentially extends the authentication methods to pass a level of assurance in the authentication context rather than attributes sent. The desired outcome of the test was to simply pass the LoA value to a properly configured SP, not to truly assert compliance. To this end the outcome passed Silver assurance without verifying the assurance.

Implementation Steps

Metadata

Update the IdP metadata with the following extension.

```
<md:Extensions xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata">
    <mdattr:EntityAttributes xmlns:mdattr="urn:oasis:names:tc:SAML:metadata:attribute">
        <saml:Attribute
            xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
            NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"
            Name="urn:oasis:names:tc:SAML:attribute:assurance-certification">
            <saml:AttributeValue>http://id.incommon.org/assurance/silver-test</saml:AttributeValue>
            <saml:AttributeValue>http://id.incommon.org/assurance/bronze-test</saml:AttributeValue>
        </saml:Attribute>
    </mdattr:EntityAttributes>
</md:Extensions>
```

Login Handler

Modify the login handler in $IDP_HOME/conf/handler.xml

```
<LoginHandler xsi:type="UsernamePassword"
              jaasConfigurationLocation="file:///opt/shibboleth-idp/conf/login.config">
    <AuthenticationMethod>urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport</AuthenticationMethod>
    <AuthenticationMethod>
      http://id.incommon.org/assurance/bronze-test
    </AuthenticationMethod>
    <AuthenticationMethod>
       http://id.incommon.org/assurance/silver-test
    </AuthenticationMethod>
</LoginHandler>
```

Servlet Configuration

Add the following servlet and servlet-mapping to the IdP web.xml and redeploy web app.

```
<servlet>
    <servlet-name>AuthnContextAuthHandler</servlet-name>
    <servlet-class>edu.internet2.middleware.shibboleth.idp.authn.provider.AuthnContextLoginServlet</servlet-class>
    <!-- Use one param for each classref that applies
         The name is an authn context reference.
         The value is an attribute_name that the remote user must have a resolved value for.
      -->
    <init-param>
        <param-name>http://id.incommon.org/assurance/bronze-test</param-name>
        <param-value>authbronze</param-value>
    </init-param>
    <init-param>
        <param-name>http://id.incommon.org/assurance/silver-test</param-name>
        <param-value>authnsilver</param-value>
```

```
        </init-param>
    </servlet>
    <servlet-mapping>
        <servlet-name>AuthnContextAuthHandler</servlet-name>
        <url-pattern>/Authn/UWLoginSilver</url-pattern>
    </servlet-mapping>
```

Test Results

Using the CiLogin test site we were able submit the silver-test assurance when requested.

uwm_saml_doc/incommon_silver_testing_use_case_zero.txt · Last modified: 2011/11/30 11:03 by mhouser