IdP Configuration for Username-Password with Silver Assurance

Background

The configurations below are for an Identity Provider wanting to use Username/Password authentication and return Silver assurance. In the first configuration, the IdP is configured to **always** return Silver assurance. In the second configuration, the IdP returns Silver assurance if the Service Provider requests Silver assurance; but if the SP does not request Silver assurance, the IdP returns PasswordProtectedTransport.

Note: The examples presented here were tested with Shibboleth IdP software version 2.3.8.

Note 2: In the XML code examples below, there is an intentional typo in URLs, with a space between "`http`" and the colon "`:`" (i.e., "`http :`"). This is because the Confluence XML formatter strangely hides URLs from display. I have circumvented this issue by adding a space in the examples. Do not copy the space in your configuration files.

Configuration 1: IdP Always Returns Silver Assurance

In the Shibboleth IdP software v.2.3.8, the UsernamePassword `<LoginHandler>` returns a single `<AuthenticationMethod>`. By default, "`urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport`" is returned. This can be changed to Silver as follows.

First, modify `web.xml` (either the `WEB-INF/web.xml` file in the deployed `war/idp.war` file, or in `shibboleth-identityprovider-2.3.8/src/main/webapp/WEB-INF/web.xml` and then redeploy `idp.war`) by adding an `<init-param>` section as follows.

```
<!-- In WEB-INF/web.xml -->

    <!-- Servlet for doing Username/Password authentication -->
    <servlet>
        <servlet-name>UsernamePasswordAuthHandler</servlet-name>
        <servlet-class>edu.internet2.middleware.shibboleth.idp.authn.provider.UsernamePasswordLoginServlet<
/servlet-class>
        <load-on-startup>3</load-on-startup>
        <init-param>
            <param-name>authnMethod</param-name>
            <param-value>http ://id.incommon.org/assurance/silver</param-value>
        </init-param>
    </servlet>
```

Then in `conf/handler.xml` (under the IdP installation directory), add a Silver assurance `<AuthenticationMethod>` to the UsernamePassword `<LoginHandler>` as follows.

```
<!-- In conf/handler.xml -->

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

You will need to redeploy `idp.war` since `web.xml` has been modified.

Configuration 2: IdP Returns Silver Assurance Only When Asked

In this configuration, the IdP returns Silver when the SP asks for Silver assurance, but returns the default PasswordProtectedTransport when the SP does NOT request Silver. For this functionality, we duplicate the original (unmodified) Username/Password sections in `web.xml` and `handler.xml` and modify the duplicated sections to be specific to Silver. Both configurations use the same Username/Password Login page, but the new section handles Silver, while the original section handles PasswordProtectedTransport (as well as no specific authentication method requested by the SP).

First, modify `web.xml` by duplicating the unmodified Username/Password section, and then making modifications for Silver. Both sections are shown below for completeness.

```
<!-- In WEB-INF/web.xml -->

    <!-- Servlet for doing Username/Password authentication -->
    <servlet>
        <servlet-name>UsernamePasswordAuthHandler</servlet-name>
        <servlet-class>edu.internet2.middleware.shibboleth.idp.authn.provider.UsernamePasswordLoginServlet<
/servlet-class>
        <load-on-startup>3</load-on-startup>
    </servlet>

    <servlet-mapping>
        <servlet-name>UsernamePasswordAuthHandler</servlet-name>
        <url-pattern>/Authn/UserPassword</url-pattern>
    </servlet-mapping>

    <!-- Servlet for doing Username/Password Silver authentication -->
    <servlet>
        <servlet-name>UsernamePasswordSilverAuthHandler</servlet-name>
        <servlet-class>edu.internet2.middleware.shibboleth.idp.authn.provider.UsernamePasswordLoginServlet<
/servlet-class>
        <load-on-startup>3</load-on-startup>
        <init-param>
          <param-name>authnMethod</param-name>
          <param-value>http ://id.incommon.org/assurance/silver</param-value>
        </init-param>
    </servlet>

    <servlet-mapping>
        <servlet-name>UsernamePasswordSilverAuthHandler</servlet-name>
        <url-pattern>/Authn/UserPasswordSilver</url-pattern>
    </servlet-mapping>
```

In the new section above, <servlet-name> (in two places) and <url-pattern> were modified by adding "Silver" to the text. Also, the <init-param> section was added to return Silver assurance by default.

Then modify conf/handler.xml by duplicating the unmodified UsernamePassword <LoginHandler> section, and then making modifications for Silver. Both sections are shown below for completeness.

```
<!-- In conf/handler.xml -->

    <!--  Username/password login handler -->
    <ph:LoginHandler xsi:type="ph:UsernamePassword"
                     jaasConfigurationLocation="file:///opt/shibboleth-idp/conf/login.config">
        <ph:AuthenticationMethod>urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport</ph:
AuthenticationMethod>
    </ph:LoginHandler>

    <!--  Username/password Silver login handler -->
    <ph:LoginHandler xsi:type="ph:UsernamePassword"
                     jaasConfigurationLocation="file:///opt/shibboleth-idp/conf/login.config"
                     authenticationServletURL="/Authn/UserPasswordSilver">
        <ph:AuthenticationMethod>http ://id.incommon.org/assurance/silver</ph:AuthenticationMethod>
    </ph:LoginHandler>
```

In the new section above, a new parameter "authenticationServletURL" was added to match the <url-pattern> entry in the web.xml. Also the <AuthenticationMethod> was changed to Silver to match the <init-param> section in the web.xml.

You will need to redeploy idp.war since web.xml has been modified.