University of Toronto

The following MCB config files show the configuration of username/password authentication via Kerberos/JAAS and the SafeNet eTokenPASS OTP product. The 'example' labels describe the customized configurations.

multi-context-broker.xml:

```
 <?xml version="1.0" encoding="UTF-8"?>
<MultiContextBroker>

    <velocityPropertiesFile>/local/shibboleth-idp/conf/velocity.properties</velocityPropertiesFile>

    <!--
        Show this list of choices for initial authentication to establish a session. Optionally limit the
choices
        to those also requested by the SP. If no choices match the SP request, then show the entire list just
as if
        the SP had not requested any.
    -->

    <!-- example: IdP displays a menu with the following choices. -->
    <initialAuthContext requestedOnly="false">
            <context name="urn:oasis:names:tc:SAML:2.0:ac:classes:Password" />
            <context name="http://id.incommon.org/assurance/bronze" />
    </initialAuthContext>

    <!--
        This value identifies the ID of the attribute in the Shibboleth attribute-resolver.xml file that
contains the user's allowed context values.
    -->

    <!-- example: IdP can obtain a value for the attribute name given below -->
    <idms attributeResolverID="eduPersonAssurance" />

    <!--
        If set to FALSE, then if the user has no assigned contexts and the SP does not request one, then
        successful authentication via the initial authentication will be returned to the SP as
        successful. This in effect mimics the current Shibboleth behavior.
        If set to TRUE, then a valid context for the user is always required.
    -->
    <principalAuthnContextRequired>true</principalAuthnContextRequired>

    <!--
        The maximum number of failures allowed a user before returning a SAML failure to the
        relying party. Must be specified according to schema definition. Set to a value of -1
        to allow an unlimited number of login failures.
     -->
    <maxFailures>3</maxFailures>

    <!--
        authContexts is the list of configured contexts the MCB will honor.
     -->
    <authnContexts>
        <!--
            For each context, the name attribute is used to match up with the values returned by the IdMS and
also
            used to match the requested authentication context sent by the SP.
            The method attribute corresponds to the authentication method this context uses.
         -->
        <context name="urn:oasis:names:tc:SAML:2.0:ac:classes:Password" method="password">
            <allowedContexts>
                <context name="http://id.incommon.org/assurance/bronze" />
            </allowedContexts>
        </context>

        <context name="http://id.incommon.org/assurance/bronze" method="bronze">
            <!--
                Note that since the bronze level allows silver and silver allows gold, means gold is acceptable
here. Contexts
```

```
                are inherited. Since two levels of silver have been configured, either is acceptable for
authenticating at the
                bronze level (but only because both are listed).
            -->
            <allowedContexts>
                <context name="http://id.incommon.org/assurance/silver" />
                <context name="http://id.incommon.org/assurance/silver-token" />
                <!--
                <context name="urn:oasis:names:tc:SAML:2.0:ac:classes:X509" />
                -->
            </allowedContexts>
        </context>

        <context name="http://id.incommon.org/assurance/silver" method="silver">
            <!--
                allowedContexts is a list of contexts which satisfy this level as well
             -->
            <allowedContexts>
                <context name="http://id.incommon.org/assurance/silver-token" />
            </allowedContexts>
        </context>

        <context name="urn:oasis:names:tc:SAML:2.0:ac:classes:X509" method="token">
            <!--
                allowedContexts is a list of contexts which satisfy this level as well
             -->
            <allowedContexts>
                <context name="edu:internet2:middleware:assurance:mcb:tokenpluspin" />
            </allowedContexts>
        </context>

        <context name="edu:internet2:middleware:assurance:mcb:tokenpluspin" method="tokenpluspin" />


    </authnContexts>

    <!--
        authMethods is the list of authentication methods supported by the MCB
     -->
    <authMethods>
        <!--
            A method defines one authentication method. The name attribute corresponds to the method value
            used in the context definition. The bean attribute is the name of the submodule bean loaded by
            the Spring framework during Shibboleth startup. The value of the method node is the friendly name
            used for display purposes.
        -->
        <method name="password" bean="mcb.usernamepassword">
            Username/Password Only
        </method>
        <method name="bronze" bean="mcb.usernamepasswordbronze">
            Username/OTP
        </method>
        <method name="silver" bean="mcb.usernamepasswordsilver">
            Silver Assurance Level
        </method>
        <method name="token" bean="mcb.token">
            Silver Assurance Level (via hardware token)
        </method>
        <method name="tokenpluspin" bean="mcb.tokenpluspin">
            Gold Level - Token/PIN Required
        </method>

    </authMethods>
</MultiContextBroker>
```

mcb-spring.xml:

```
 <?xml version="1.0" encoding="UTF-8"?>
<beans xmlns="http://www.springframework.org/schema/beans" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
```

```
    xmlns:util="http://www.springframework.org/schema/util"
    xsi:schemaLocation="http://www.springframework.org/schema/beans http://www.springframework.org/schema/beans
/spring-beans-2.0.xsd
                        http://www.springframework.org/schema/util http://www.springframework.org/schema/util
/spring-util-2.0.xsd">

    <!-- This bean represents an authentication submodule -->
    <!-- Example: Configures the use of Kerberos to do password authentication -->
    <bean id="mcb.usernamepassword" class="edu.internet2.middleware.assurance.mcb.authn.provider.
JAASLoginSubmodule">
        <constructor-arg index="0" value="/local/shibboleth-idp/conf/login.config.mcb" />
        <constructor-arg index="1" value="MCBUserPassAuth" />
        <constructor-arg index="2" value="jaaslogin.vm" />
    </bean>

    <!-- This bean represents an authentication submodule -->
    <!-- Example: Configures the use of the SafeNet eTokenPass OTP device using the RADIUS JAAS Module from
Pieter Vandepitte -->
    <bean id="mcb.usernamepasswordbronze" class="edu.internet2.middleware.assurance.mcb.authn.provider.
JAASLoginSubmodule">
        <constructor-arg index="0" value="/local/shibboleth-idp/conf/login.config.radius" />
        <constructor-arg index="1" value="MCBUserOTPAuth" />
        <constructor-arg index="2" value="jaasloginbronze.vm" />
    </bean>

    <!-- This bean represents an authentication submodule -->
    <bean id="mcb.usernamepasswordsilver" class="edu.internet2.middleware.assurance.mcb.authn.provider.
JAASLoginSubmodule">
        <constructor-arg index="0" value="/local/shibboleth-idp/conf/login.config.mcb" />
        <constructor-arg index="1" value="MCBUserPassAuth" />
        <constructor-arg index="2" value="jaasloginsilver.vm" />
    </bean>

    <!-- This bean represents an authentication submodule -->
    <!--
    <bean id="mcb.token" class="edu.internet2.middleware.assurance.mcb.authn.provider.TokenLoginSubmodule">
    </bean>
    -->

    <!-- Example: Configure the use of the remote_user login handler for X.509 certs -->
    <bean id="mcb.token" class="edu.internet2.middleware.assurance.mcb.authn.provider.RemoteUserSubmodule">
        <!-- <constructor-arg index="0" value="/Authn/MCB/RemoteUser" /> -->
        <constructor-arg index="0" value="/Authn/X509/Login" />
    </bean>


    <!-- This bean is our configuration object representing the custom configuration file -->
    <bean id="mcb.Configuration" class="edu.internet2.middleware.assurance.mcb.authn.provider.MCBConfiguration">
        <constructor-arg
            value="/local/shibboleth-idp/conf/multi-context-broker.xml" />
        <constructor-arg>
            <list>
                <ref bean="mcb.usernamepassword" />
                <ref bean="mcb.usernamepasswordbronze" />
                <ref bean="mcb.usernamepasswordsilver" />
                <ref bean="mcb.token" />
            </list>
        </constructor-arg>

    </bean>

    <!-- This bean places the configuration bean into the Servlet space -->
    <bean id="mcb.ServletAttributeExporter" class="edu.internet2.middleware.shibboleth.common.config.service.
ServletContextAttributeExporter"
        depends-on="mcb.Configuration" init-method="initialize">
        <constructor-arg>
            <list>
                <value>mcb.Configuration</value>
            </list>
        </constructor-arg>
    </bean>
```

```
</beans>
```