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

       default-init-method="initialize"
       default-destroy-method="destroy">

    <!--
    This file provisions the IdP with information about the configured login mechanisms
    available for use.
    The actual beans and subflows that make up those mechanisms are in their own files, but
    this pulls them
    together with deployer-supplied metadata to describe them to the system.

    You can turn on and off individual mechanisms by adding and remove them here. Nothing
    left out will
    be used, regardless any other files loaded by the Spring container.

    Flow defaults include: no support for IsPassive/ForceAuthn, support for non-browser
    clients enabled,
    and default timeout and lifetime values set via properties. We also default to
    supporting the SAML 1/2
    expressions for password-based authentication over a secure channel, so anything more
    exotic requires
    customization, as the example below for IP address authentication illustrates.
    -->

    <util:list id="shibboleth.AvailableAuthenticationFlows">

         <!-- Ajout pour ShibCAS -->
         <bean id="authn/Shibcas" parent="shibboleth.AuthenticationFlow"
                p:passiveAuthenticationSupported="true"
                p:forcedAuthenticationSupported="true"
                p:nonBrowserSupported="false" />
        <!-- Fin de Ajout pour ShibCAS -->

        <bean id="authn/IPAddress" parent="shibboleth.AuthenticationFlow"
                p:passiveAuthenticationSupported="true"
                p:lifetime="PT60S" p:inactivityTimeout="PT60S">
            <property name="supportedPrincipals">
                  <list>
                    <bean parent="shibboleth.SAML2AuthnContextClassRef"
                        c:classRef="urn:oasis:names:tc:SAML:2.0:ac:classes:InternetProtocol"
                        />

                </list>
            </property>
        </bean>

<bean id="authn/SPNEGO" parent="shibboleth.AuthenticationFlow"
                p:nonBrowserSupported="false">
            <property name="supportedPrincipals">
                <list>
                    <bean parent="shibboleth.SAML2AuthnContextClassRef"
                        c:classRef="urn:oasis:names:tc:SAML:2.0:ac:classes:Kerberos" />
                    <bean parent="shibboleth.SAML1AuthenticationMethod"
                        c:method="urn:ietf:rfc:1510" />
                </list>
```

```
            </property>
        </bean>
        <bean id="authn/External" parent="shibboleth.AuthenticationFlow"
            p:nonBrowserSupported="false" />

        <bean id="authn/RemoteUser" parent="shibboleth.AuthenticationFlow"
            p:nonBrowserSupported="false" />

        <bean id="authn/RemoteUserInternal" parent="shibboleth.AuthenticationFlow" />

        <bean id="authn/X509" parent="shibboleth.AuthenticationFlow"
                p:nonBrowserSupported="false">
            <property name="supportedPrincipals">
                <list>
                    <bean parent="shibboleth.SAML2AuthnContextClassRef"
                        c:classRef="urn:oasis:names:tc:SAML:2.0:ac:classes:X509" />
                    <bean parent="shibboleth.SAML2AuthnContextClassRef"
                        c:classRef="urn:oasis:names:tc:SAML:2.0:ac:classes:TLSClient" />
                    <bean parent="shibboleth.SAML1AuthenticationMethod"
                        c:method="urn:ietf:rfc:2246" />
                </list>
            </property>
        </bean>

        <bean id="authn/X509Internal" parent="shibboleth.AuthenticationFlow">
            <property name="supportedPrincipals">
                <list>
                    <bean parent="shibboleth.SAML2AuthnContextClassRef"
                        c:classRef="urn:oasis:names:tc:SAML:2.0:ac:classes:X509" />
                    <bean parent="shibboleth.SAML2AuthnContextClassRef"
                        c:classRef="urn:oasis:names:tc:SAML:2.0:ac:classes:TLSClient" />
                    <bean parent="shibboleth.SAML1AuthenticationMethod"
                        c:method="urn:ietf:rfc:2246" />
                </list>
            </property>
        </bean>
    <!--
        <bean id="authn/Password" parent="shibboleth.AuthenticationFlow"
                p:passiveAuthenticationSupported="true"
                p:forcedAuthenticationSupported="true" />-->

    <!-- Ajout steve test -->
                <bean id="authn/Password" parent="shibboleth.AuthenticationFlow"
                p:passiveAuthenticationSupported="true"
                p:forcedAuthenticationSupported="true" >
            <property name="supportedPrincipals">
                <list>
                    <bean parent="shibboleth.SAML2AuthnContextClassRef"
                        c:classRef=
                        "http://schemas.microsoft.com/ws/2008/06/identity/authenticationmethod
                        /password" />
                </list>
            </property>

        </bean>
<!-- Ajout steve test -->

    </util:list>

    <!--
    This is a map used to "weight" particular methods above others if the IdP has to
    randomly select one
    to insert into a SAML authentication statement. The typical use shown below is to bias
    the IdP in favor
    of expressing the SAML 2 PasswordProtectedTransport class over the more vanilla Password
    class on the
    assumption that the IdP doesn't accept passwords via an insecure channel. This map never
    causes the IdP
```

```
    to violate its matching rules if an RP requests a particular value; it only matters when
    nothing specific
    is chosen. Anything not in the map has a weight of zero.
    -->

    <util:map id="shibboleth.AuthenticationPrincipalWeightMap">
        <entry>
            <key>
                <bean parent="shibboleth.SAML2AuthnContextClassRef"
                    c:classRef=
                    "urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport" />
            </key>
            <value>1</value>
        </entry>
    </util:map>

</beans>
```