Ministerio de Modernización
Presidencia de la Nación

Integración con PAEC desde una aplicación JAVA

En este punto se describe la creación de un cliente Java desplegado en WildFly y securizado con keycloak.json.

PAEC define un nuevo método de autenticación para las aplicaciones, llamado KEYCLOAK. Este método reemplaza al método actual, configurado en el archivo web.xml (que puede ser BASIC, FORM, etc.). Sin embargo, corresponde al servidor de aplicaciones interpretar éste método. Por eso, es necesario instalar un adaptador en él, que de otro modo mostrará un error de "método de autenticación desconocido".

Existen distintos adaptadores para distintos servidores. Los mismos se pueden descargar desde el sitio de Keycloak (http://www.keycloak.org/). Como PAEC está construido sobre Keycloak 3.2.1.Final, es compatible con los adaptadores de esa versión. Además, hay dos juegos de adaptadores: el primero para el protocolo OpenID Connect, y el segundo para el protocolo SAML.

La aplicación necesita datos sobre PAEC, para poder redirigir al usuario cuando quiera autenticarse o cerrar sesión. Estos datos se encuentran en el archivo keycloak.json, que personal de Ministerio entregará al equipo desarrollador de la aplicación cliente de PAEC (previa descarga desde la pestaña "Instalación" del cliente como se indicó más arriba).

1. En el archivo web.xml de la aplicación web, se deberán agregar las restricciones de seguridad:

```
<!-- Conexion a PAEC -->
<security-constraint>
    <web-resource-collection>
        <url-pattern>/*</url-pattern>
    </web-resource-collection>
        <auth-constraint>
        <role-name>(rol del usuario)</role-name>
        </auth-constraint>
</security-constraint>
<login-config>
        <auth-method>KEYCLOAK</auth-method>
        <realm-name>(nombre del dominio)</realm-name>
</login-config>
<security-role>
        <role-name>(rol del usuario)</role-name>
</security-role>
```

Esto securiza todas las URLs de la aplicación con PAEC. Notar que es necesario usar como restricción por lo menos un rol.

1. Agregar las librerías necesarias para recuperar los datos de PAEC. Si es un proyecto Maven, las dependencias son:

```
        <!-- HTTP -->
        <dependency>
        <groupId>org.apache.httpcomponents</groupId>
        <artifactId>httpclient</artifactId>
        <version>4.5.3</version>
        </dependency>

        <!-- JSON -->
        <dependency>
        <groupId>org.codeartisans</groupId>
        <artifactId>org.json</artifactId>
        <version>20150729</version>
        </dependency>

        <!-- Keycloak -->
        <dependency>
        <groupId>org.keycloak</groupId>
        <artifactId>keycloak-core</artifactId>
        <version>3.2.1.Final</version>
        </dependency>

    <dependency>
        <groupId>org.keycloak</groupId>
        <artifactId>keycloak-adapter-core</artifactId>
        <version>3.2.1.Final</version>
        <scope>provided</scope>
        </dependency>
```

1. Para obtener datos acerca de Tramix Identity en la aplicación, referirse al código en la aplicación de ejemplo adjunto "java-app".
2. Pegar el archivo keycloak.json entregado previamente por personal del Ministerio en el directorio WEB-INF de la aplicación.

Integración con PAEC desde un cliente Java vía Application Server

En este punto se describe la creación de un cliente PAEC desplegado en un servidor JBoss y securizado por keycloak-subsystem.

Cuando la aplicación Java se despliega sobre un servidor JBoss, se puede securizar el WAR directamente en el servidor. Los pasos a seguir son los mismos, exceptuando la instalación del archivo keycloak.json.

En la consola de administración, en la ficha del cliente, pestaña Instalación, elegir “Keycloak OIDC JBoss Subsystem XML”. Esto genera un snippet XML. Pegarlo en el archivo standalone.xml o domain.xml (según corresponda), dentro del subsistema “keycloak”:

```
<profile>
        ...
        <subsystem xmlns="urn:jboss:domain:keycloak:1.1">
    <secure-deployment name="cliente-app.war">
       ...
    </secure-deployment>
        </subsystem>
        …
</profile>
```

Cambiar el nombre del WAR por el correspondiente al de la aplicación. Es necesario reiniciar el servidor para que los cambios tomen efecto.

Adaptador Keycloak en el servidor de aplicaciones Wildfly

Servidor de aplicaciones WildFly

Para instalar el adaptador en WildFly, los pasos son los siguientes:

1. Descomprimir el adaptador en el directorio del servidor.
2. Configurar el subsistema en el archivo standalone.xml:
3. Agregar el subsistema en la sección extensions:

```
<extensions>
        <extension module="org.keycloak.keycloak-adapter-subsystem"/>
        …
</extensions>
```

1. Agregar la extensión en el perfil:

```
<profile>
        <subsystem xmlns="urn:jboss:domain:keycloak:1.1"/>
        …
</profile>
```

1. Agregar el dominio de seguridad en el subsistema correspondiente:

```
<subsystem xmlns="urn:jboss:domain:security:1.2">
        <security-domains>
        …
        <security-domain name="keycloak">
        <authentication>
                <login-module
code="org.keycloak.adapters.jboss.KeycloakLoginModule" flag="required"/>
        </authentication>
        </security-domain>
        </security-domains>
```

Esto instala el subsistema "keycloak-subsystem". Este módulo de WildFly permite securizar aplicaciones con el método KEYCLOAK.