Argentina Presidencia

PAEC - Integración de aplicaciones .NET 4.X

1. Introducción

La integración de nuevas aplicaciones a PAEC implica tres tipos de cambios, todos dependiendo de la tecnología de la aplicación y del servidor en que se ejecuta:

1) Configuración del reino y del cliente en PAEC.
2) Adaptación en el servidor.
3) Adaptación en la aplicación.

2. Configuración de Aplicaciones

Las aplicaciones cliente deben ser modificadas, teniendo en cuenta los siguientes aspectos:

1. Configuración del cliente
2. Restricción de acceso a páginas securizadas
3. Obtención de datos del usuario logueado
4. Logout

2.1. .NET

La adaptación de una webapp .NET para ser securizada con PAEC consta de agregar la autenticación con OpenID Connect, modificar en el código la obtención de datos de usuario para leerlos desde PAEC y modificar los links de cierre de sesión, para que hagan un logout en

PAEC.

.NET Framework 4.X

Instalar y utilizar paquete Owin.Security.Keycloak-3 https://www.nuget.org/packages/Owin.Security.Keycloak-3 Validar la existencia de los paquetes: https://www.nuget.org/packages/Microsoft.Owin.Security/ https://www.nuget.org/packages/Microsoft.Owin.Security.Cookies

1. Startup.cs

Agregar autenticación con OpenID Connect a la aplicación

```
using Microsoft.Owin; using
Microsoft.Owin.Security; using
Microsoft.Owin.Security.Cookies; using
Owin; using Owin.Security.Keycloak; using
     System;            using
System.Web.Configuration;


[assembly: OwinStartup(typeof(StandardFlow.Startup))] namespace
StandardFlow
{     public class Startup
    {     const string persistentAuthType =
CookieAuthenticationDefaults.AuthenticationType;    public void
Configuration(IAppBuilder app)
       {            app.UseCookieAuthentication(new
CookieAuthenticationOptions
               {
                      AuthenticationType = persistentAuthType
               });


               app.SetDefaultSignInAsAuthenticationType(persistentAuthType);


               app.UseKeycloakAuthentication(new KeycloakAuthenticationOptions
               {
                      Realm = WebConfigurationManager.AppSettings["RealmId"],
                      ClientId = WebConfigurationManager.AppSettings["ClientId"],
                      ClientSecret =
WebConfigurationManager.AppSettings["ClientSecret"],
                      KeycloakUrl =
WebConfigurationManager.AppSettings["Authority"],
                      AuthenticationType = persistentAuthType,
                      SignInAsAuthenticationType = persistentAuthType,
                      AllowUnsignedTokens = false,
                      DisableIssuerSigningKeyValidation = false,
                      DisableIssuerValidation = false,
                      DisableAudienceValidation = false,
               });    TokenClockSkew = TimeSpan.FromSeconds(2)
```

```
        }
    }   }
```

2. Web.config

Agregar variables de configuración

```
<configuration>    <appSettings>
...
       <add key="ClientId" value="client-id"/>
       <add key="ClientSecret" value="client-secret"/>
       <add key="RealmId" value="realm-id"/>  <add key="Authority"
       value="https://tst.autenticar.gob.ar/auth"/>  ...
}
```

Donde, *client-id* es el identificador del cliente en PAEC, *client-secret* es el secreto del cliente (si es requerido por la configuración en PAEC) y *realm-id* es el identificador del reino en PAEC.

3. *Controller.cs

Agregar anotación de autorización a los Controller o métodos que requieran autenticación

```
[Authorize] public class
HomeController : Controller { ...
```

4. Obtener usuario autenticado

User.Identity.Name

5. Cerrar sesión

Para cerrar sesión, redirigir a:
http://tst.autenticar.gob.ar/auth/realms/<realmid>/protocol/openidconnect/logout?redirect_uri=http://server/app/close-session

Donde, *realm-id* es el identificador del reino en PAEC y *http://server/app/close-session* es la url para cerrar y limpiar la sesión de la aplicación.