**OpenID Connect**

OIDC在OAuth的基础上扩展了一些新的概念

1. ID Tokens

ID Token是一个签名的JWT，它包含一组关于用户身份的声明（claim），如：用户的标识（sub）、颁发令牌的提供程序的标识符（iss）、创建此标识的Client标识（aud）等

我们可以使用ID Token来做身份认证，而不需要使用access\_token。不过，OIDC为了保持于OAuth的兼容，会同时提供Id token和access\_token。

1. UserInfo Endpoint

OIDC还提供了一个包含当前用户信息的标准的受保护的资源。

OIDC中定义了一个特殊的openid scope，并且是必须的，它包含对Id token和UserInfo Endpoint的访问权限。

1. Hybrid Flow

混合流模式是授权码模式与隐式模式的组合，在一次请求中可以同时获取Code和ID Token，ResponseType可以是：code id\_token, code id\_token token 和 code token。

下面介绍ASP.NET Core 中的OIDC认证

添OpenIdConnect的Nuget包：Microsoft.AspNetCore.Authentication.OpenIdConnect

OIDC的注册其实要比OAuth还简单些：

services.AddAuthentication(options =>

{

    // 授权Scheme使用Cookie

    options.DefaultAuthenticateScheme = CookieAuthenticationDefaults.AuthenticationScheme;

    // 登录Scheme使用Cookie

    options.DefaultSignInScheme = CookieAuthenticationDefaults.AuthenticationScheme;

    // 未登录跳转使用OIDC

    options.DefaultChallengeScheme = OpenIdConnectDefaults.AuthenticationScheme;

})

// 添加Cookie Scheme

.AddCookie()

// 添加OIDC Scheme

.AddOpenIdConnect(o =>

{

    o.ClientId = "oidc.hybrid";

    o.ClientSecret = "secret";

    // 若不设置Authority，就必须指定MetadataAddress

    o.Authority = "https://oidc.faasx.com/";

    // 默认为Authority+".well-known/openid-configuration"

    //o.MetadataAddress = "https://oidc.faasx.com/.well-known/openid-configuration";

o.RequireHttpsMetadata = false;

    // 使用混合流

    o.ResponseType = OpenIdConnectResponseType.CodeIdToken;

    // 是否将Tokens保存到AuthenticationProperties中

    o.SaveTokens = true;

    // 是否从UserInfoEndpoint获取Claims

    o.GetClaimsFromUserInfoEndpoint = true;

    // 在本示例中，使用的是IdentityServer，而它的ClaimType使用的是JwtClaimTypes。

o.TokenValidationParameters.NameClaimType = "name"; //JwtClaimTypes.Name;

    // 以下参数均有对应的默认值，通常无需设置。

    //o.CallbackPath = new PathString("/signin-oidc");

    //o.SignedOutCallbackPath = new PathString("/signout-callback-oidc");

    //o.RemoteSignOutPath = new PathString("/signout-oidc");

    //o.Scope.Add("openid");

    //o.Scope.Add("profile");

//o.ResponseMode = OpenIdConnectResponseMode.FormPost;

    /\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*相关事件\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*/

    // 未授权时，重定向到OIDC服务器时触发

//o.Events.OnRedirectToIdentityProvider = context => Task.CompletedTask;

    // 获取到授权码时触发

    //o.Events.OnAuthorizationCodeReceived = context => Task.CompletedTask;

    // 接收到OIDC服务器返回的认证信息（包含Code, ID Token等）时触发

    //o.Events.OnMessageReceived = context => Task.CompletedTask;

    // 接收到TokenEndpoint返回的信息时触发

    //o.Events.OnTokenResponseReceived = context => Task.CompletedTask;

    // 验证Token时触发

    //o.Events.OnTokenValidated = context => Task.CompletedTask;

    // 接收到UserInfoEndpoint返回的信息时触发

    //o.Events.OnUserInformationReceived = context => Task.CompletedTask;

    // 出现异常时触发

//o.Events.OnAuthenticationFailed = context => Task.CompletedTask;

    // 退出时，重定向到OIDC服务器时触发

    //o.Events.OnRedirectToIdentityProviderForSignOut = context => Task.CompletedTask;

    // OIDC服务器退出后，服务端回调时触发

    //o.Events.OnRemoteSignOut = context => Task.CompletedTask;

    // OIDC服务器退出后，客户端重定向时触发

//o.Events.OnSignedOutCallbackRedirect = context => Task.CompletedTask;

});

**运行流程**

1. 登录

我们访问受保护资源，将会被重定向至授权服务器

请求：

GET http://localhost:5002/profile HTTP/1.1

响应：

HTTP/1.1 302 Found

Location: https://oidc.faasx.com/connect/authorize?client\_id=oidc.hybrid&redirect\_uri=http://localhost:5002/signin-oidc&response\_type=code id\_token&scope=openid profile&response\_mode=form\_post&nonce=636428853279287956.N2IxZmFlZDgtNDNmZC00OTRmLTljMWItNTVjMmQwOTVjNTQ3MWUyMDcxNTctZDg4Yy00MDRiLThmNmQtYjE1YTdjOGE4MThm&state=CfDJ8B4XRZETkRhMt3mT9VduB8LSACJO9seruKlM3kYPxaRyWcUSt0BvPMd6RUGAiay8qraTWLdMh9B3ClRJDE-BtMRYTmzGJSHegueIW-fyq2G9TpUtSQCd23BxAYrdB4SeGQte2IXaQ82cKMz-aSHQ7TTzhPO\_fgDtIVlwDJBtwgKQzEkEyyLsfH2DHxwr\_Ojn3M-uRHId2bi9RF2gR\_1hqoTdYlv-CZodFKuUGSMCqJO4cZLsuuAb-PrSnamz7h7MOpPixIOgQq5gd25sxF8avpSTsoT5HbU2fCiqX7g3rbCLzMG-rTnDftN8uZRiqc-JcyGkLPGIoj-FLNoW\_yfZbGk&x-client-SKU=ID\_NET&x-client-ver=2.1.4.0

Set-Cookie: .AspNetCore.OpenIdConnect.Nonce.CfDJ8B4XRZETkRhMt3mT9VduB8IHI9Q\_BeT6uPrlI72UUqej78UfqAdiczZsPOxF3Gy7bSm7Swh9Jh0\_haVi-UnQxUTGq-9xQLcaMX-PuXMjf6-6sLqc15NUgoLQ1w3KWqjkt7-3NlYW4qka6LqDPRtWJxT7vICtPhjx8ecNWtW\_ijqBg\_W8osmZLvFGS3PzPipP1UF14AkaIp48dFV1qNqt67Yta8ebXH7SHGkUhfcA5R-O0B8t-Q7sWL4NTN8AdKQF02HMqs\_duf-4FLf2p7Rbpsc=N; expires=Fri, 06 Oct 2017 11:30:27 GMT; path=/signin-oidc; httponly

Set-Cookie: .AspNetCore.Correlation.OpenIdConnect.BqW1filmAVCStL92ghXFQZBoLQjG5-Gl\_m60zxCW9BA=N; expires=Fri, 06 Oct 2017 11:30:27 GMT; path=/signin-oidc; httponly

重定向地址中包含如下几个参数：

client\_id 客户端标识

redirect\_uri 回调地址

response\_type 授权类型

scope 权限范围

response\_mode 响应模式

nonce OIDC服务器会在identity token中包含此参数

state 用于保存状态，会原封不动地返回

1. 在OIDC服务器登录成功后，授权服务器返回一个自动提交的表单，其目标是我们填写的回调地址

<form method='post' action='http://localhost:5002/signin-oidc'>

<input type='hidden' name='code' value='eb53860906da276a1bb5318c5d539db085c6ca1fd3467da9d918aa7524f20f63' />

<input type='hidden' name='id\_token' value='eyJhbGciOiJSUzI1NiIsImtpZCI6IjdlYzk5MjVlMmUzMTA2NmY2ZmU2ODgzMDRhZjU1ZmM0IiwidHlwIjoiSldUIn0.eyJuYmYiOjE1MDcyODg1MjcsImV4cCI6MTUwNzI4ODgyNywiaXNzIjoiaHR0cDovL29pZGMuZmFhc3guY29tIiwiYXVkIjoib2lkYy5oeWJyaWQiLCJub25jZSI6IjYzNjQyODg1MzI3OTI4Nzk1Ni5OMkl4Wm1GbFpEZ3RORE5tWkMwME9UUm1MVGxqTVdJdE5UVmpNbVF3T1RWak5UUTNNV1V5TURjeE5UY3RaRGc0WXkwME1EUmlMVGhtTm1RdFlqRTFZVGRqT0dFNE1UaG0iLCJpYXQiOjE1MDcyODg1MjcsImNfaGFzaCI6ImJNT1FNVGdDV3VMX25EbHo5MDU4M3ciLCJzaWQiOiJjZTVjODg2ZmFhZDFiNTc4MDVkNzExYjkzZTliYWQ0ZiIsInN1YiI6IjAwMSIsImF1dGhfdGltZSI6MTUwNzI4ODM5NSwiaWRwIjoibG9jYWwiLCJhbXIiOlsicHdkIl19.BBn0SigvOW9USk-Mi1WP\_lJPWI9I06gsuomhqp69Ip5y3kqFyiBCVanzULsR4fBa0tOOBOtcPJzAfivzLqsMRwW1QfRamfVIlXuuzcRsR8WP1pFxvFPekwKi-D6-RLmmQzUT-\_78WvboiAu\_dZtwe0cm4ZLDCJH6LLCPs2xXTHYuNI7YoyAgeGKDAhWle0VrsbdlrcubPPgQFfFXPdLDInnLr8eEMpUZ7nru0FJgxm3Ah4hGXPKMud8jhLUMXDcSaKseL8tDgxIowmhpXOknU-y9x5FlrZUFOReDxaBZe7DG5V0xsPrdhMxMkZQbHHz8cJoaYrqcwHClm8rScEPxVA' />

<input type='hidden' name='scope' value='openid profile' />

<input type='hidden' name='state' value='CfDJ8B4XRZETkRhMt3mT9VduB8LSACJO9seruKlM3kYPxaRyWcUSt0BvPMd6RUGAiay8qraTWLdMh9B3ClRJDE-BtMRYTmzGJSHegueIW-fyq2G9TpUtSQCd23BxAYrdB4SeGQte2IXaQ82cKMz-aSHQ7TTzhPO\_fgDtIVlwDJBtwgKQzEkEyyLsfH2DHxwr\_Ojn3M-uRHId2bi9RF2gR\_1hqoTdYlv-CZodFKuUGSMCqJO4cZLsuuAb-PrSnamz7h7MOpPixIOgQq5gd25sxF8avpSTsoT5HbU2fCiqX7g3rbCLzMG-rTnDftN8uZRiqc-JcyGkLPGIoj-FLNoW\_yfZbGk' />

<input type='hidden' name='session\_state' value='g0m\_0W2scFKHxVQP\_8jdNt48r2XV8wDlF\_\_-ST9aYtk.28e1d34baad6d122a92c667329084600' />

</form>

<script>(function(){document.forms[0].submit();})();</script>

如上，可以看到，表单中包含有id\_token，因为我们使用的是code id\_token类型

1. 退出

退出时，我们现在本地退出，然后重定向到授权服务器执行退出

请求报文：

GET http://localhost:5002/signout-remote HTTP/1.1

Cookie: .AspNetCore.Cookies=xxx

响应报文：

HTTP/1.1 302 Found

Location: http://oidc.faasx.com/connect/endsession?post\_logout\_redirect\_uri=http://localhost:5002/signout-callback-oidc&id\_token\_hint=eyJhbGciOiJSUzI1NiIsImtpZCI6IjdlYzk5MjVlMmUzMTA2NmY2ZmU2ODgzMDRhZjU1ZmM0IiwidHlwIjoiSldUIn0.eyJuYmYiOjE1MDc0MjgzMTAsImV4cCI6MTUwNzQyODYxMCwiaXNzIjoiaHR0cDovL29pZGMuZmFhc3guY29tIiwiYXVkIjoib2lkYy5oeWJyaWQiLCJub25jZSI6IjYzNjQzMDI1MTExOTUyNjYxNS5NVFU0WXpNMFl6RXRZemcwWmkwME5UWTFMVGcyTW1ZdE5XUmtZbUZtTUdabU5UWXlaalF6TkRReE9HWXROalEwWXkwMFpHTmtMVGhqTlRFdE1XWTROV0V3TW1NM09UZG0iLCJpYXQiOjE1MDc0MjgzMTAsImF0X2hhc2giOiJQSHRvd1JrUHhYLWNsclBzRnYxMkpnIiwic2lkIjoiMzFmMWJmMTA1MTU4MmZjMGE3ZTZhZjFjY2I0Y2RlMzUiLCJzdWIiOiIwMDEiLCJhdXRoX3RpbWUiOjE1MDc0MjgzMTAsImlkcCI6ImxvY2FsIiwiYW1yIjpbInB3ZCJdfQ.hIxkDhsx\_WE6IxM68O7uqkqdQquXXnOtxhlnrYiBJuU7Ex\_aApVXoKUdHS8HMx1nLswntr6SRsrygyMJnGMdzP5JutGsmfO\_i1WYGqk3BlTD7ry0wfBd\_U9OaVFcJhcVZq4q5u3SA47Wxqex9vifiHrTBQFT\_l6JqpevRLn-y91IxTl9rnXKfrHowhPsHJjdLzda3Lyj0wWWtb2N\_ng19mRChmDd4RXucP9mBHdQDyLZtvIJ5iIzV4pqtL7VCylFzV4RBLbCzUeuRnHI3E\_MqTaGWvVyFbUAKpr55TmVoc6lAOS4ie4CPzilR52KLWZ4l9eQh-WeIOA3NBgzHlJigg&state=CfDJ8B4XRZETkRhMt3mT9VduB8IbG5c9um6S\_maiHLsMKlIFRVtKMyLuXfqgB6e1OhWWVVJDYbgedt6hmyi1ny2aMbKW-SgHTru73YezUAZpre2ELXM3trlnX3YW\_FTkcGE\_RUyaR3hQ3eEYFmMdgdZdf0M&x-client-SKU=ID\_NET&x-client-ver=2.1.4.0

其中id\_token\_hint为id\_token