Integration of Microsoft® .NET Framework / Core with DoubleClue using OpenID

1. Introduction

This guide is intended for developers of .NET Framework / Core applications who use OpenID / OAuth for authentication and want to integrate DoubleClue Multi-Factor Authentication (MFA) into their product.

Requirements:

- .NET Framework application with Microsoft.Owin installed OR .NET Core web application.
- DoubleClue Enterprise Management (DCEM) installation with registered users.

2. Preparing DCEM to be an OpenID Authentication Server

In order to prepare DCEM to be an Authentication Server, please see chapter <chapter> of "DCEM_Manual_EN.pdf".

3. Registering the application as an OpenID Client for DCEM

1. In DCEM, go to main menu item "OpenID-OAuth", sub menu "Client Metadata".
2. Click "Add".
3. Enter a Display Name for ease of identification.
4. Enter your Client ID if you have one, or click "Generate" to create one.
5. Enter your Client Secret if you have one, or click "Generate" to create one.
6. Click "OK".

Your application is now registered as an OpenID client for DCEM.

4. Connecting a .NET Framework web application with DCEM

Add these settings into the Configuration method of your OWIN Startup class.

```
app.UseOpenIdConnectAuthentication(new OpenIdConnectAuthenticationOptions
{
    ClientId = clientId,
    ClientSecret = clientSecret,
    Authority = tokenUri,
    RedirectUri = redirectUri,
    ResponseType = OpenIdConnectResponseType.CodeIdTokenToken,
    Scope = OpenIdConnectScope.OpenIdProfile,
    TokenValidationParameters = new TokenValidationParameters
    {
        IssuerSigningKey = new SymmetricSecurityKey(Encoding.UTF8.GetBytes(clientSecret))
    },
    Notifications = new OpenIdConnectAuthenticationNotifications
    {
        AuthorizationCodeReceived = async n =>
        {
            HttpClient client = new HttpClient();

            // Get Access Token
            TokenResponse tokenResponse = await client.RequestAuthorizationCodeTokenAsync(
                new AuthorizationCodeTokenRequest
            {
                Address = tokenUri,
                ClientId = clientId,
                ClientSecret = clientSecret,
                RedirectUri = redirectUri,
                Code = n.Code
            });
            if (tokenResponse.IsError) throw new Exception(tokenResponse.Error);

            // Get User Claims
            UserInfoResponse userInfoResponse = await client.GetUserInfoAsync(new UserInfoRequest
            {
                Address = userInfoUri,
                Token = tokenResponse.AccessToken
            });
            if (userInfoResponse.IsError) throw new Exception(userInfoResponse.Error);

            n.AuthenticationTicket.Identity.AddClaims(userInfoResponse.Claims);
        },
    },
});
```

- ***clientId*** is the Client ID registered in DCEM
- ***clientSecret*** is the Client Secret registered in DCEM
- ***tokenUri*** is the URL set in the Issuer field of the Preferences screen in DCEM's OpenID-OAuth module, along with "/dcem/oauth". For example, if the Issuer is "https://dcem:8080", the tokenUri is "https://dcem:8080/dcem/oauth".
- ***userInfoUri*** is the same as *tokenUri*, but with "/userinfo" added at the end. Using the same example, it becomes "https://dcem:8080/dcem/oauth/userinfo".
- ***redirectUri*** is a URL of your choosing within the domain of your client application. OWIN requires this to have a location where to expect Authorisation Codes and Access Tokens.

5. Connecting a .NET Core web application with DCEM

Add these settings into the Configure method of your ASP.NET Core Startup class.

```
app.UseOpenIdConnectAuthentication(new OpenIdConnectOptions
{
    SaveTokens = true,
    ClientId = clientId,
    ClientSecret = clientSecret,
    ResponseType = OpenIdConnectResponseType.Code,
    TokenValidationParameters = new TokenValidationParameters
    {
        IssuerSigningKey = new
SymmetricSecurityKey(Encoding.UTF8.GetBytes(clientSecret))
    },
    Authority = tokenUri,
});
```

- ***clientId*** is the Client ID registered in DCEM
- ***clientSecret*** is the Client Secret registered in DCEM
- ***tokenUri*** is the URL set in the Issuer field of the Preferences screen in DCEM’s OpenID-OAuth module, along with “/dcem/oauth”. For example, if the Issuer is “https://dcem:8080”, the tokenUri is “https://dcem:8080/dcem/oauth”.