Authenticate users and call protected APIs in your MAUI app

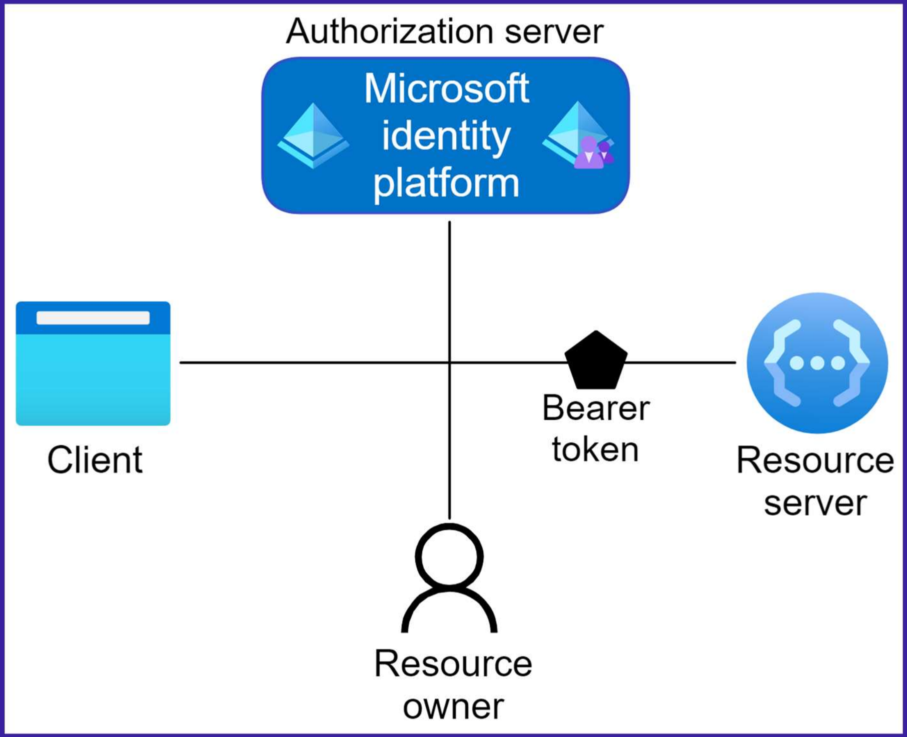
Sameer Khandekar

History of Authentication

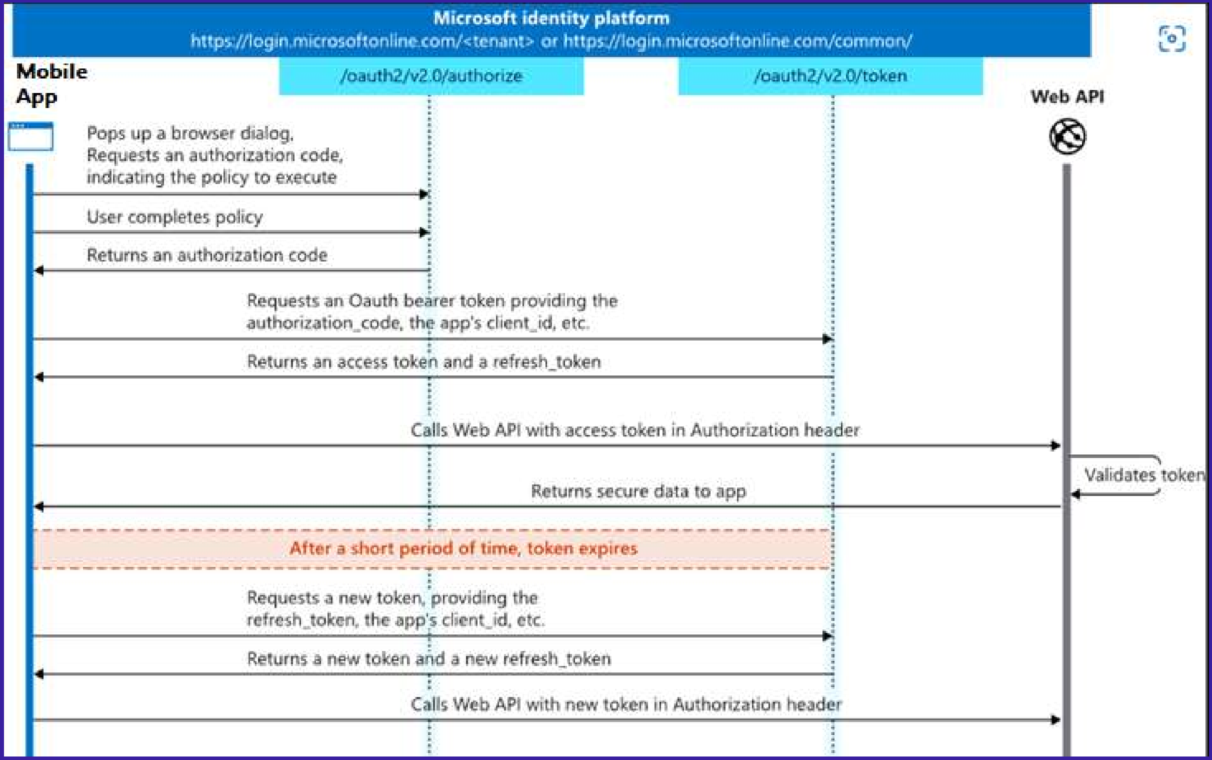
- Store username and password
  - Plain text
- Problem: No way to get data from the 3rd party other than store as plain text

What is OAuth 2.0 & OpenID Connect (OIDC)

- **High Level**
  - Scoped Access to resource
  - Private dialog between Authorization Server and User
- **Token Types**
  - AT, RT
  - IdToken



Authorization Code Flow


Microsoft identity platform
https://login.microsoftonline.com/<tenant> or https://login.microsoftonline.com/common/
Mobile App
/oauth2/v2.0/authorize
/oauth2/v2.0/token
Web API

Pops up a browser dialog, Requests an authorization code, indicating the policy to execute

User completes policy

Returns an authorization code

Requests an Oauth bearer token providing the authorization_code, the app's client_id, etc.

Returns an access token and a refresh_token

Calls Web API with access token in Authorization header

Validates token

Returns secure data to app

After a short period of time, token expires

Requests a new token, providing the refresh_token, the app's client_id, etc.

Returns a new token and a new refresh_token

Calls Web API with new token in Authorization header

MSAL.NET made it simple

- Configuration in Portal
  - https://aka.ms/mobile-app-reg
- Public Client – Desktop Apps, Mobile Apps
  - Corporate Accounts (Azure Active Directory)
  - Personal Accounts (B2C e.g. Facebook, Google, Microsoft Personal Account)
- Code – Only 3 cross platform steps
  - Create the PublicClientApplication
  - Call AcquireTokenSilent
  - If it requires UI, call AcquireTokenInteractive
- Platform specific code + redirect URIs

Demos

- Maui Basic App
- Maui App With Broker
- Maui B2C App

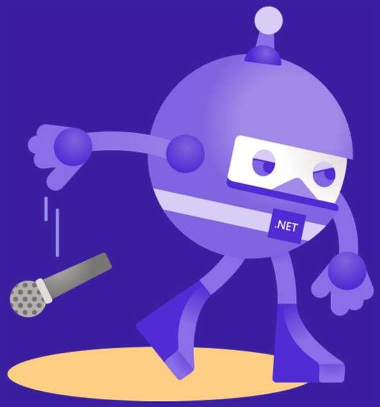
- Location: https://github.com/AzureAD/microsoft-authentication-library-for-dotnet/tree/main/tests/devapps/MauiApps

References

- NuGet - https://www.nuget.org/packages/Microsoft.Identity.Client/
- GitHub - https://github.com/AzureAD/microsoft-authentication-library-for-dotnet
- Maui Status - https://github.com/AzureAD/microsoft-authentication-library-for-dotnet/blob/main/MauiStatus.md
- Maui DevApps - https://github.com/AzureAD/microsoft-authentication-library-for-dotnet/tree/main/tests/devapps/MauiApps
- Maui DevOps - https://devblogs.microsoft.com/dotnet/devops-for-dotnet-maui/
- MSAL samples - https://docs.microsoft.com/en-us/azure/active-directory/develop/sample-v2-code
- App Types and Auth Flows - https://docs.microsoft.com/en-us/azure/active-directory/develop/authentication-flows-app-scenarios

Thanks for joining!

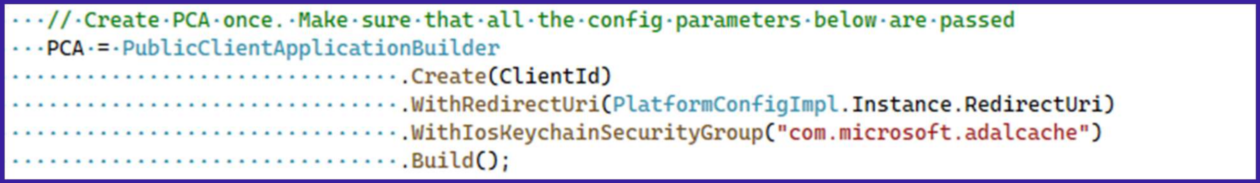
Ask your questions live on Twitter #dotNETConf



Consolidated code changes in the next slides.

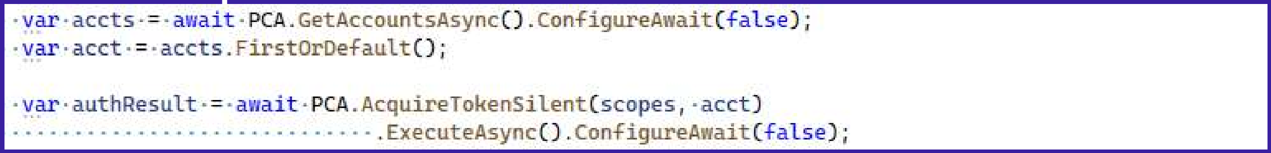
Cross Platform Code

- Create the PublicClientApplication



```
   // Create PCA once. Make sure that all the config parameters below are passed
   PCA = PublicClientApplicationBuilder
                                .Create(ClientId)
                                .WithRedirectUri(PlatformConfigImpl.Instance.RedirectUri)
                                .WithIosKeychainSecurityGroup("com.microsoft.adalcache")
                                .Build();
```

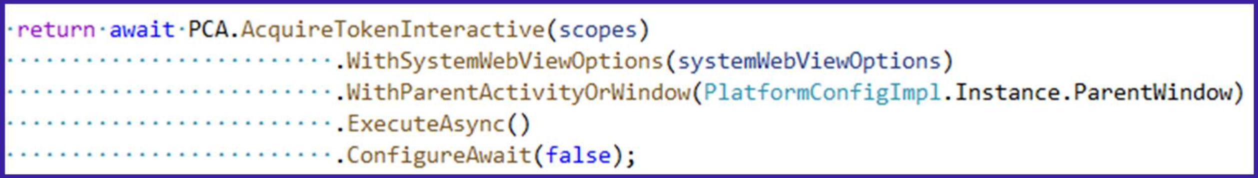
- Call AcquireTokenSilent



```
 var accts = await PCA.GetAccountsAsync().ConfigureAwait(false);
 var acct = accts.FirstOrDefault();

 var authResult = await PCA.AcquireTokenSilent(scopes, acct)
                              .ExecuteAsync().ConfigureAwait(false);
```

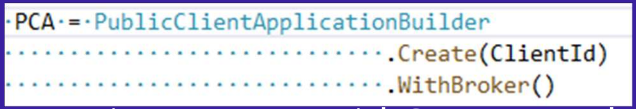
- If it requires UI, call AcquireTokenInteractive



```
 return await PCA.AcquireTokenInteractive(scopes)
                          .WithSystemWebViewOptions(systemWebViewOptions)
                          .WithParentActivityOrWindow(PlatformConfigImpl.Instance.ParentWindow)
                          .ExecuteAsync()
                          .ConfigureAwait(false);
```

Tweaks for Broker and B2C

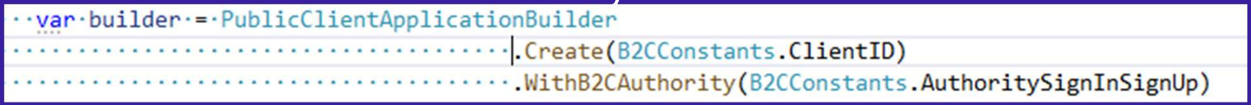
- Broker
  - Create - Add WithBroker.



```
 PCA = PublicClientApplicationBuilder
                            .Create(ClientId)
                            .WithBroker()
```

  - Interactive – Keep WithSystemWebViewOptions/WithUseEmbeddedView Used when broker is not available.

- B2C
  - Create – Add WithB2CAuthority



```
  var builder = PublicClientApplicationBuilder
                                     .Create(B2CConstants.ClientID)
                                     .WithB2CAuthority(B2CConstants.AuthoritySignInSignUp)
```

  - Silent – Add WithB2CAuthority
  - WithBroker is not applicable
  - Google B2C does not support Embedded View

Cross Platform Code – Maui Difference

- Project structure
  - Will show in the code
- Internal change: ~~AesManaged~~ -> Aes

Android Changes

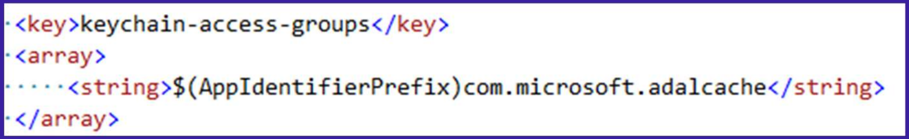
- AndroidManifest.xml
  - Add BrowserTabActivity and MsalActivity as respondent to redirect URI
- MainActivity.cs
  - OnCreate
  - OnActivityResult
- MsalActivity.cs
  - For non broker only

Android Code – Maui Difference

- Internal: ~~AndroidClientHandler~~ -> AndroidMessageHandler
- Add [Activity(Exported =true)] to Activity

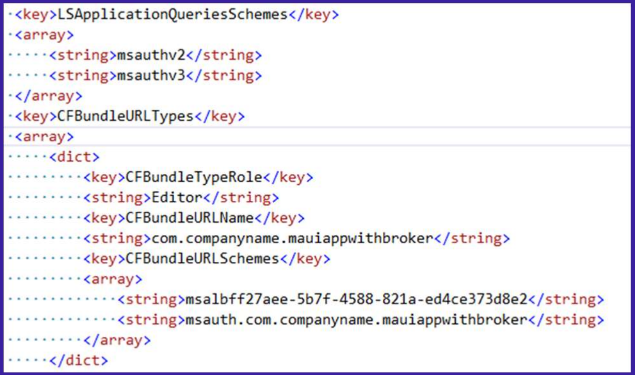
iOS Changes

- AppDelegate.cs
  - Configure Redirect URI
  - Broker Override OpentURL – Continue with AuthenticationContinuationHelper
- Entitlements.plist
  - Add



```
 <key>keychain-access-groups</key>
 <array>
     <string>$(AppIdentifierPrefix)com.microsoft.adalcache</string>
 </array>
```

- Info.plist
  - Broker – Add LSApplicationQueriesSchemes, and CFBundleURLTypes



```
 <key>LSApplicationQueriesSchemes</key>
 <array>
     <string>msauthv2</string>
     <string>msauthv3</string>
 </array>
 <key>CFBundleURLTypes</key>
 <array>
     <dict>
         <key>CFBundleTypeRole</key>
         <string>Editor</string>
         <key>CFBundleURLName</key>
         <string>com.companyname.mauiappwithbroker</string>
         <key>CFBundleURLSchemes</key>
         <array>
             <string>msalbff27aee-5b7f-4588-821a-ed4ce373d8e2</string>
             <string>msauth.com.companyname.mauiappwithbroker</string>
         </array>
     </dict>
```

iOS Changes - Maui Difference

- AppDelegate:: OpenUrl no pointer to the sourceApplication
- Specify min iOS in the project