Apps - Authentication and Authorization using Azure B2C

In the ever-evolving landscape of digital applications, security is of paramount importance. Users expect seamless and secure access to services, and developers must meet these demands while also ensuring data privacy. Azure Active Directory B2C (Azure B2C) is a powerful tool in the Microsoft Azure ecosystem that addresses these concerns by providing a comprehensive authentication and authorization solution for applications. In this blog, we will explore the problem of user authentication and authorization in apps, delve into the solution using Azure B2C, discuss the technical details, implementation, challenges, and the business benefits it offers.

Problem Statement:

User authentication and authorization are critical components of modern applications. Developers face the challenge of implementing secure and user-friendly authentication systems that can handle diverse identity providers, support multi-factor authentication (MFA), and offer customizable user experiences. Furthermore, managing user data securely and adhering to privacy regulations are complex tasks. Traditional approaches often require significant development effort and can result in suboptimal user experiences.

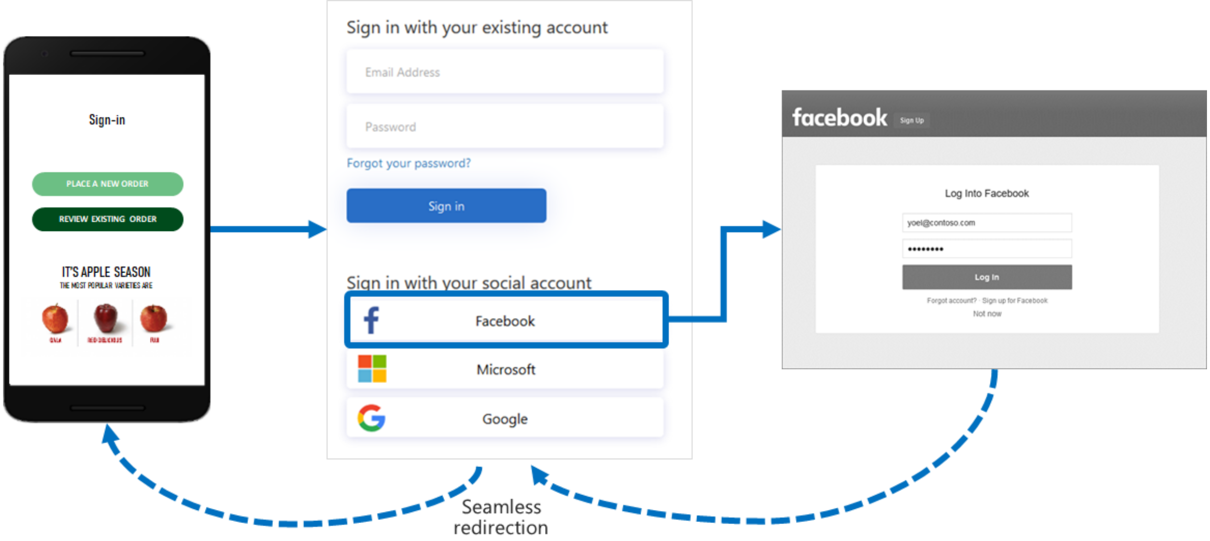
Solution/Architecture:

Azure B2C offers a robust solution for these challenges. It allows developers to add authentication and authorization to their applications with ease. Here's an overview of the architecture and code snippets to get started.

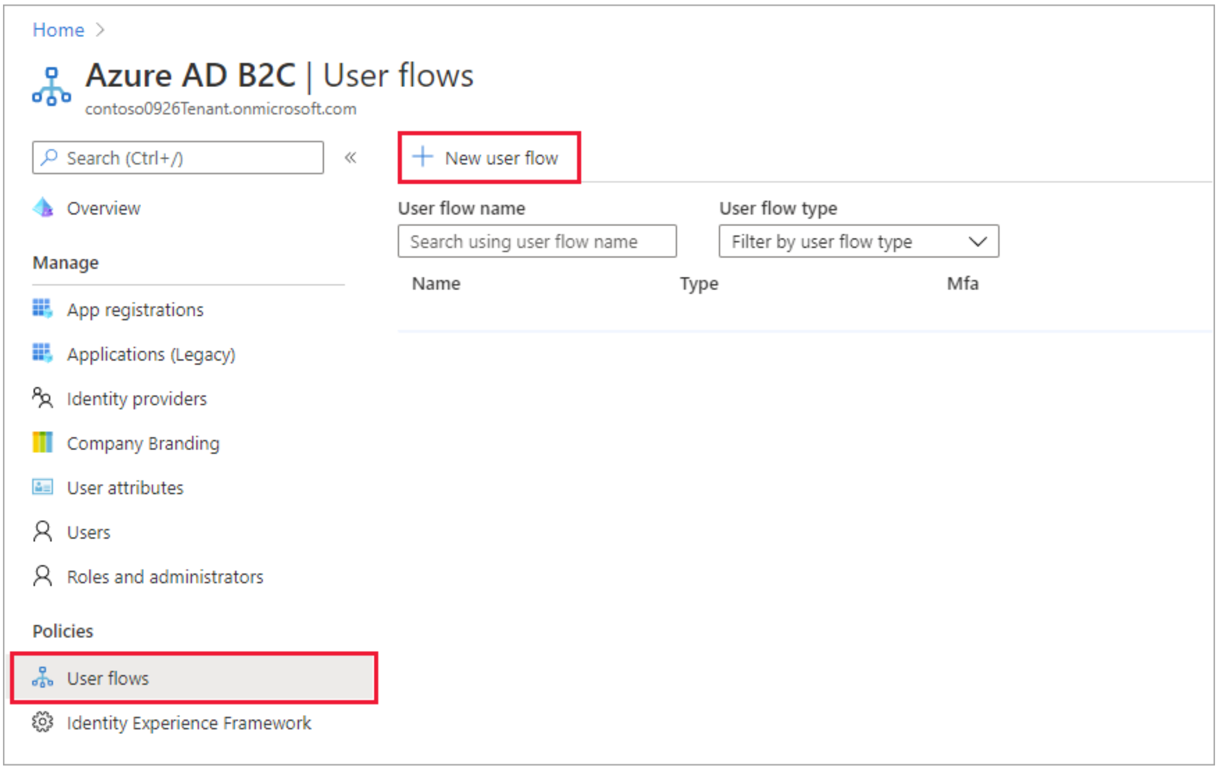
Architecture:

Azure B2C follows a flexible and scalable architecture that includes the following components:

1. **Identity Providers:** Azure B2C supports various identity providers, including social logins like Facebook, Google, and enterprise providers such as Azure AD, allowing users to sign in with their preferred accounts



2. **User Flows:** User flows define the user journey during authentication, including sign-up, sign-in, profile editing, and password reset. These can be customized to match your app's look and feel.



Home >

Azure AD B2C | User flows

contoso0926Tenant.onmicrosoft.com

Search (Ctrl+/)

Overview

Manage

- App registrations
- Applications (Legacy)
- Identity providers
- Company Branding
- User attributes
- Users
- Roles and administrators

Policies

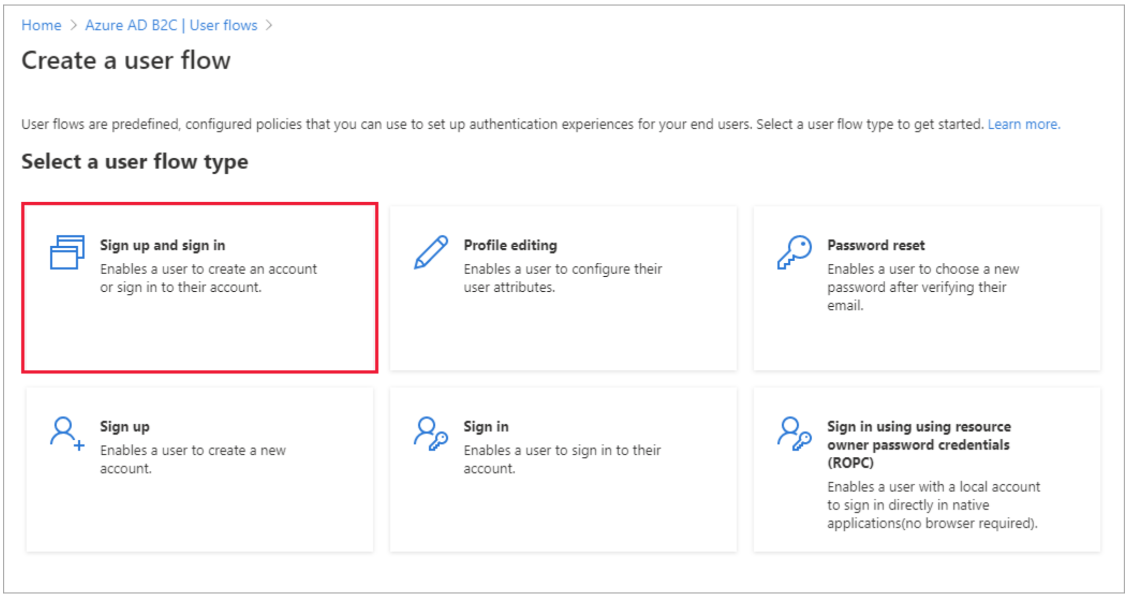
- User flows
- Identity Experience Framework

+ New user flow

User flow name: Search using user flow name

User flow type: Filter by user flow type

Name	Type	Mfa



Home > Azure AD B2C | User flows >

Create a user flow

User flows are predefined, configured policies that you can use to set up authentication experiences for your end users. Select a user flow type to get started. Learn more.

Select a user flow type

Sign up and sign in
Enables a user to create an account or sign in to their account.

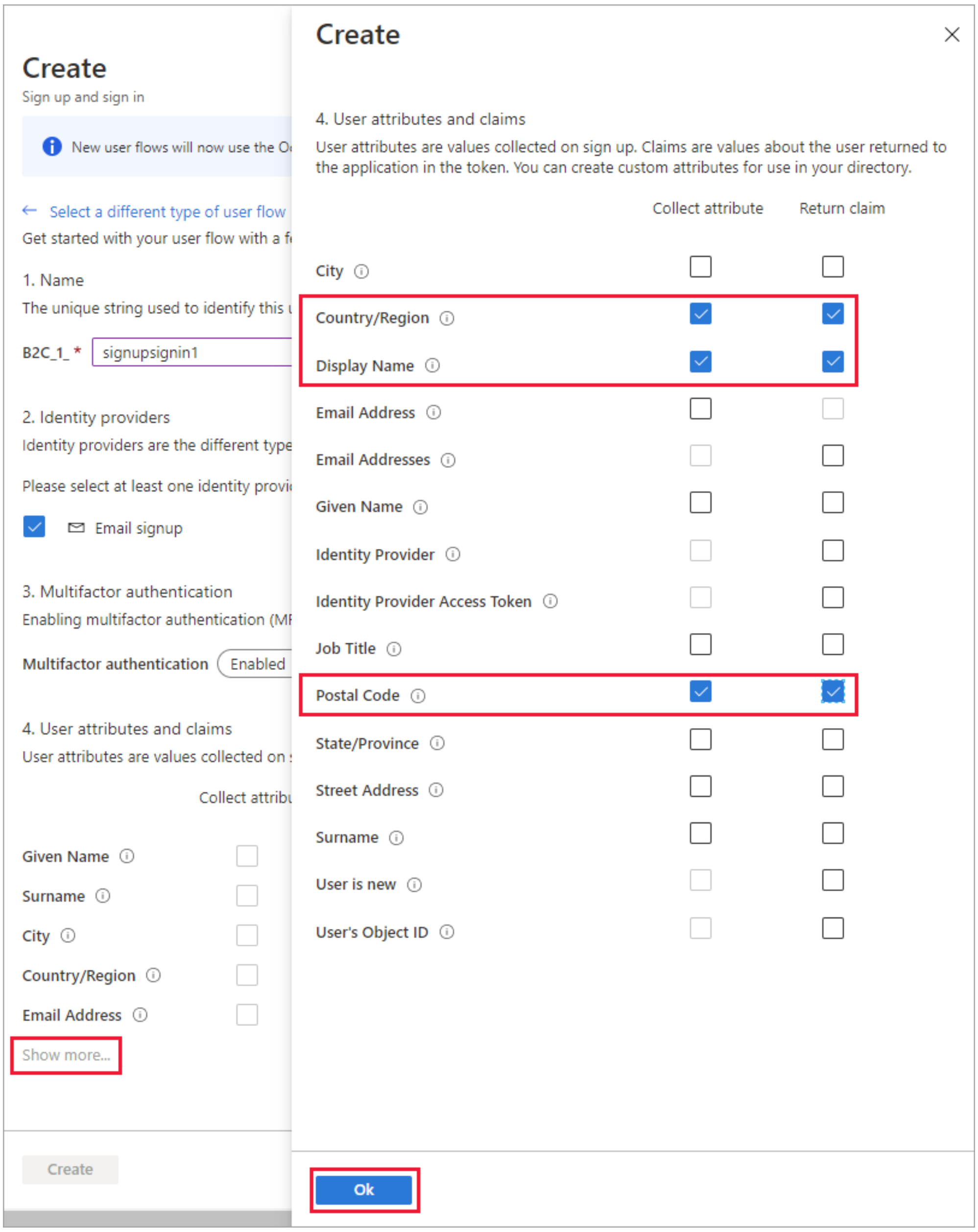
Profile editing
Enables a user to configure their user attributes.

Password reset
Enables a user to choose a new password after verifying their email.

Sign up
Enables a user to create a new account.

Sign in
Enables a user to sign in to their account.

Sign in using using resource owner password credentials (ROPC)
Enables a user with a local account to sign in directly in native applications(no browser required).



Create
Sign up and sign in

New user flows will now use the O

← Select a different type of user flow

Get started with your user flow with a f

1. Name

The unique string used to identify this u

B2C_1_ * signupsignin1

2. Identity providers

Identity providers are the different type

Please select at least one identity provi

☑ Email signup

3. Multifactor authentication

Enabling multifactor authentication (MF

Multifactor authentication Enabled

4. User attributes and claims

User attributes are values collected on s

	Collect attribu
Given Name	□
Surname	□
City	□
Country/Region	□
Email Address	□

Show more...

Create

Create

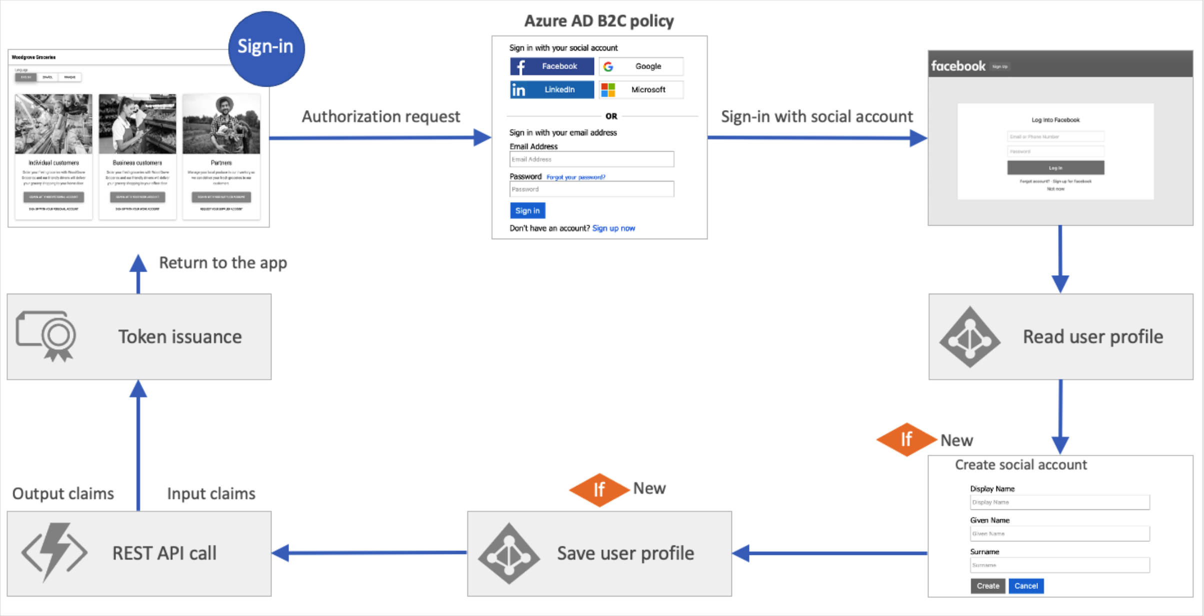
4. User attributes and claims

User attributes are values collected on sign up. Claims are values about the user returned to the application in the token. You can create custom attributes for use in your directory.

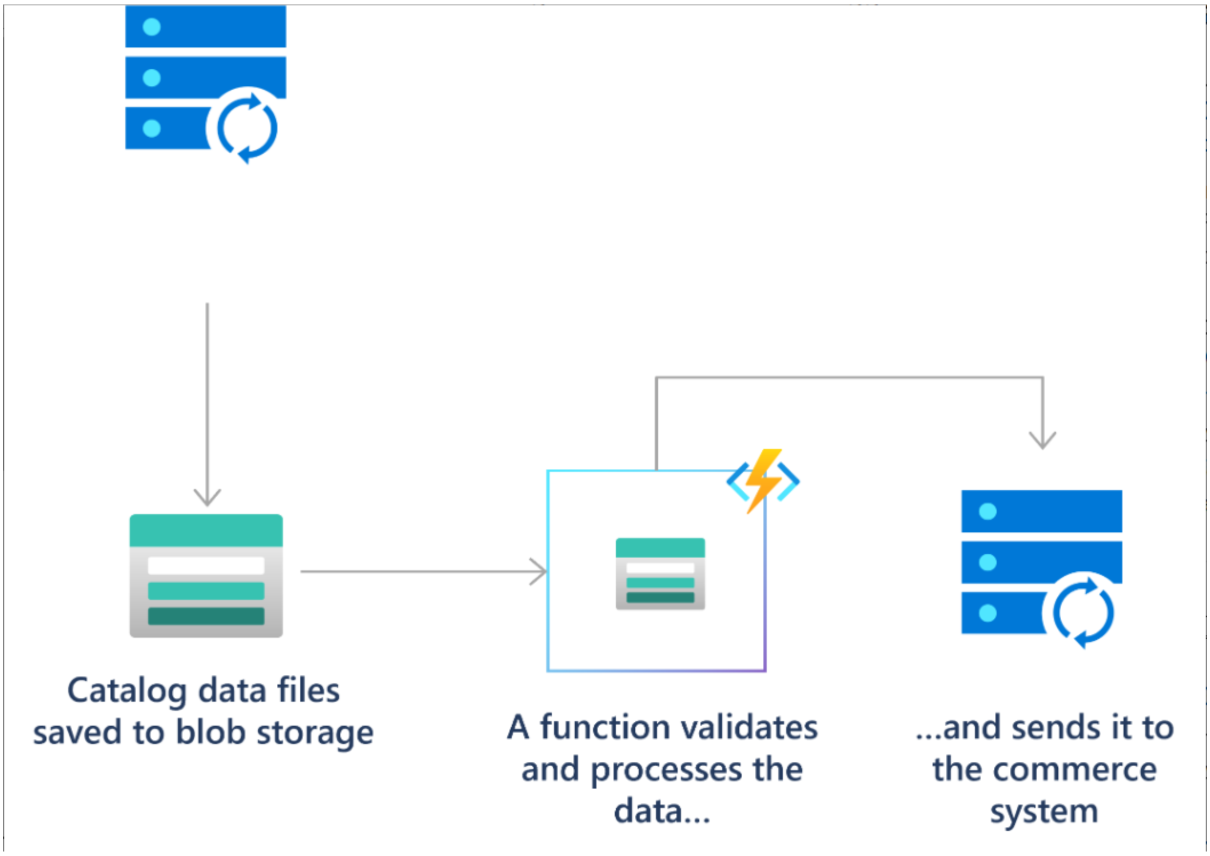
	Collect attribute	Return claim
City	□	□
Country/Region	☑	☑
Display Name	☑	☑
Email Address	□	□
Email Addresses	□	□
Given Name	□	□
Identity Provider	□	□
Identity Provider Access Token	□	□
Job Title	□	□
Postal Code	☑	☑
State/Province	□	□
Street Address	□	□
Surname	□	□
User is new	□	□
User's Object ID	□	□

Ok

3. **Custom Policies:** For advanced scenarios, custom policies can be created to define complex authentication and authorization requirements.



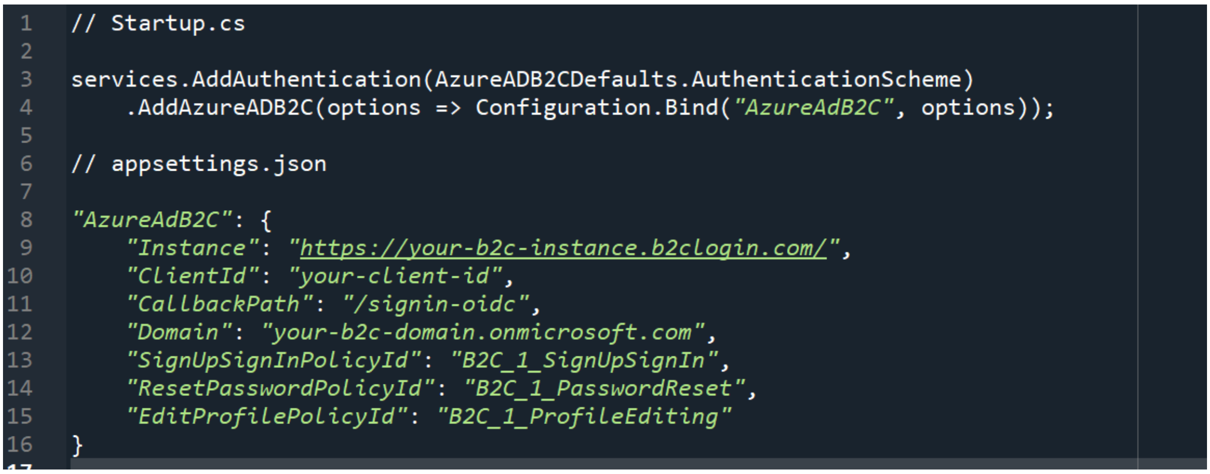
4. **Azure Functions:** Azure Functions can be integrated to execute custom logic during authentication and authorization processes.


Catalog data files saved to blob storage
A function validates and processes the data...
...and sends it to the commerce system

Code (ASP.NET Core Example):

Below is a simplified example of integrating Azure B2C authentication into an ASP.NET Core application:

#csharp

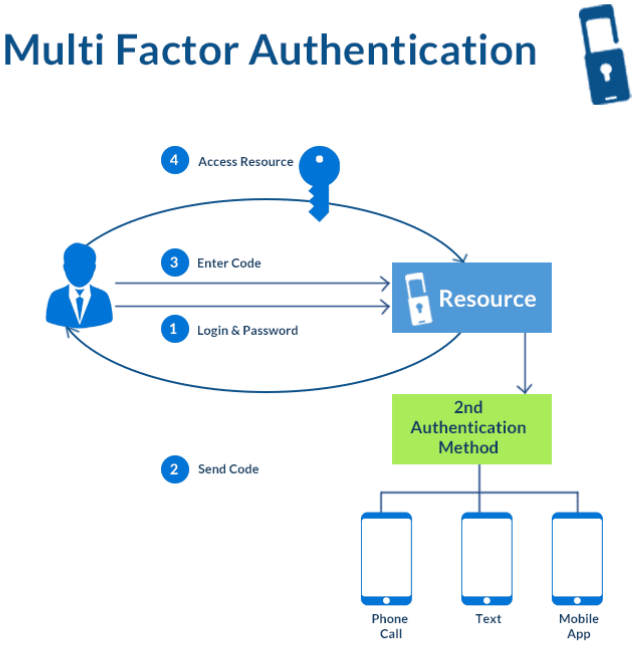


```
// Startup.cs

services.AddAuthentication(AzureADB2CDefaults.AuthenticationScheme)
    .AddAzureADB2C(options => Configuration.Bind("AzureAdB2C", options));

// appsettings.json

"AzureAdB2C": {
    "Instance": "https://your-b2c-instance.b2clogin.com/",
    "ClientId": "your-client-id",
    "CallbackPath": "/signin-oidc",
    "Domain": "your-b2c-domain.onmicrosoft.com",
    "SignUpSignInPolicyId": "B2C_1_SignUpSignIn",
    "ResetPasswordPolicyId": "B2C_1_PasswordReset",
    "EditProfilePolicyId": "B2C_1_ProfileEditing"
}
```

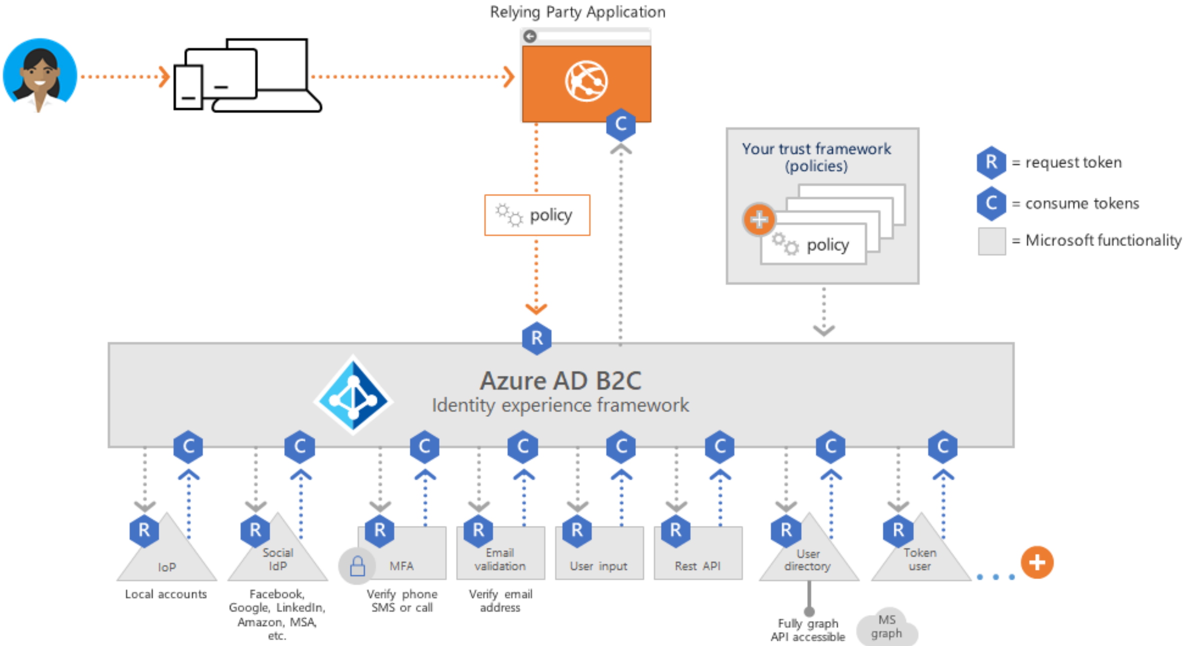
Technical Details and Implementation of Solution:

Azure B2C offers several features that enhance security and usability:

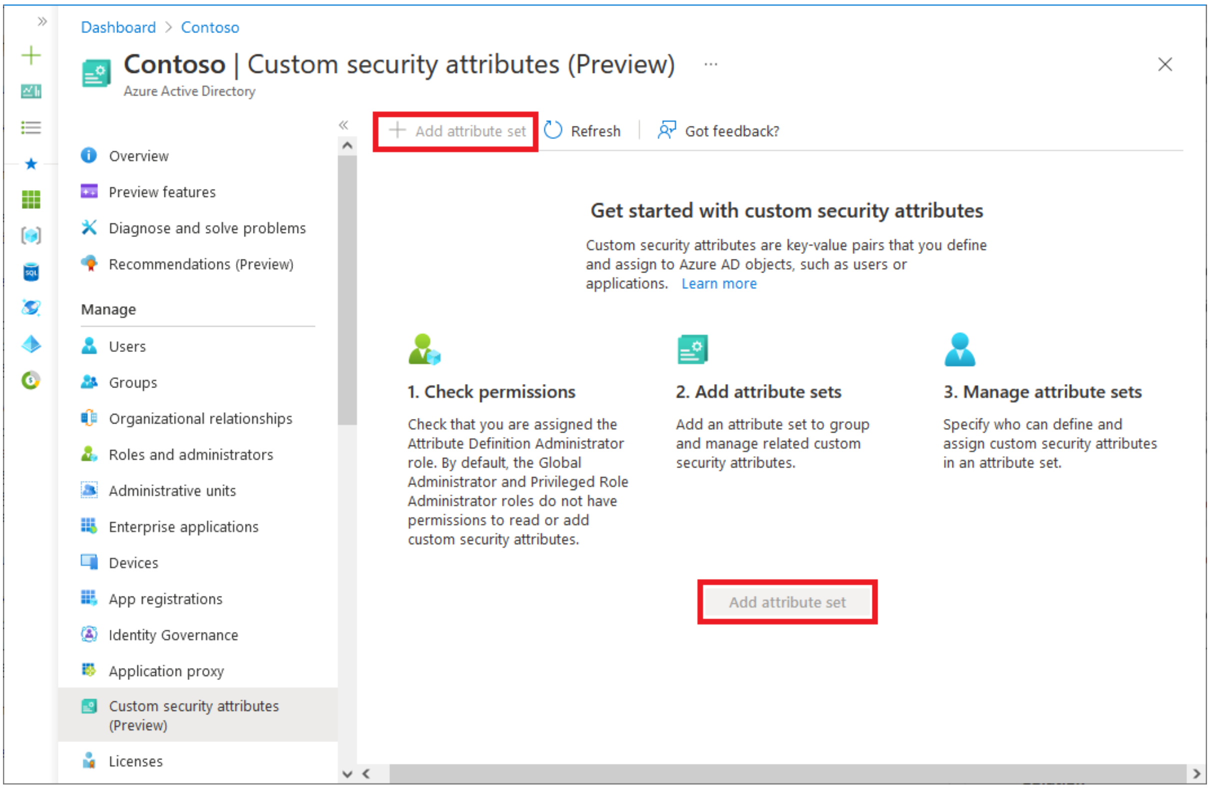
1. **Multi-Factor Authentication (MFA):** Azure B2C supports MFA, enhancing security by requiring users to verify their identity through multiple methods.



2. **Customizable User Journeys:** User flows can be customized to collect additional user data during registration or sign-in, ensuring that your app captures the required information.



3. **User Attributes and Custom Policies:** You can define custom attributes and policies to suit your app's specific requirements, such as mapping user attributes to external systems or customizing the authentication process.


Dashboard > Contoso

Contoso | Custom security attributes (Preview)

Azure Active Directory

Get started with custom security attributes

Custom security attributes are key-value pairs that you define and assign to Azure AD objects, such as users or applications. Learn more

1. Check permissions

Check that you are assigned the Attribute Definition Administrator role. By default, the Global Administrator and Privileged Role Administrator roles do not have permissions to read or add custom security attributes.

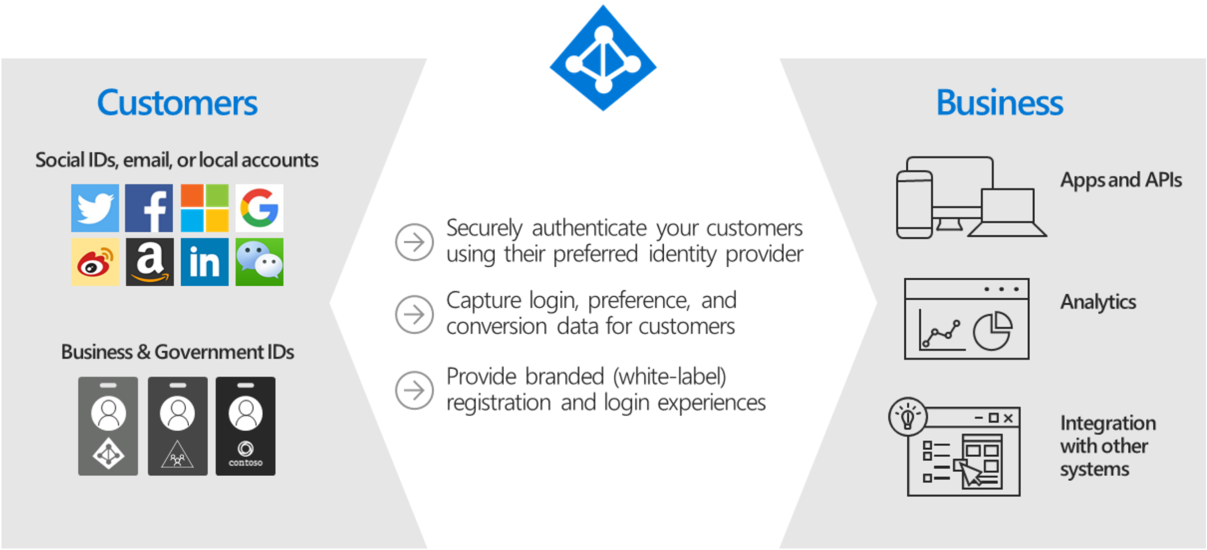
2. Add attribute sets

Add an attribute set to group and manage related custom security attributes.

3. Manage attribute sets

Specify who can define and assign custom security attributes in an attribute set.

4. **User Data Storage:** Azure B2C securely stores user profiles, reducing the complexity of managing user data.


Customers
Social IDs, email, or local accounts
Business & Government IDs
contoso
Securely authenticate your customers using their preferred identity provider
Capture login, preference, and conversion data for customers
Provide branded (white-label) registration and login experiences
Business
Apps and APIs
Analytics
Integration with other systems

Challenges in Implementing the Solution:

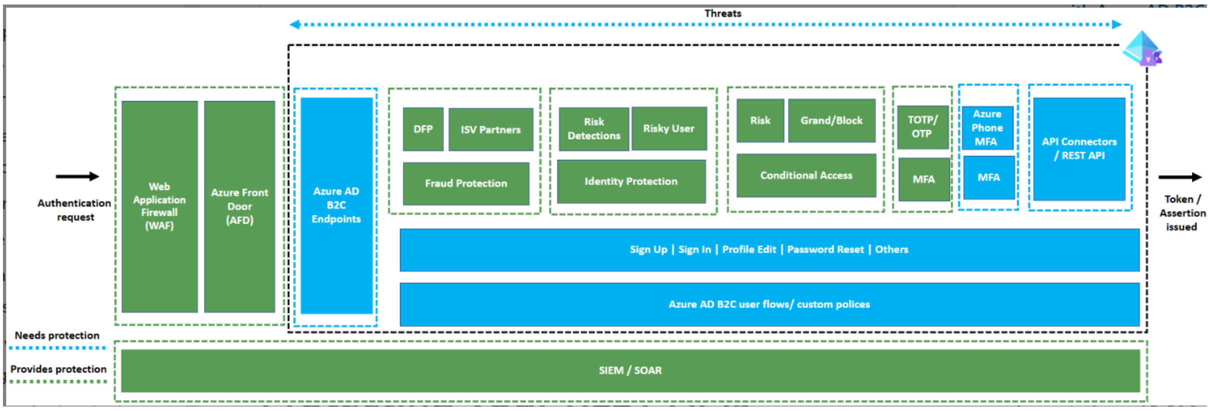
While Azure B2C offers a powerful solution, there are some challenges to consider:

1. **Learning Curve:** Getting familiar with Azure B2C's features and configuration options may take time for developers who are new to the platform.
2. **Customization Complexity:** While customization is a strength, complex customization scenarios may require expertise in policy configuration.
3. **Cost:** Azure B2C is a paid service, and the cost can vary depending on the number of users and transactions.

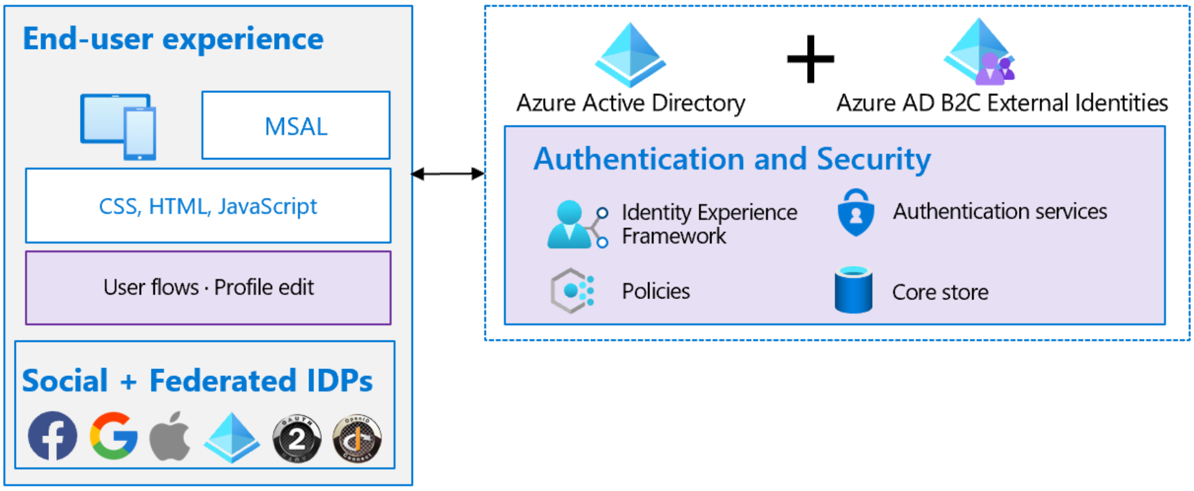
Business Benefit:

Implementing Azure B2C for authentication and authorization in your applications brings several business benefits:

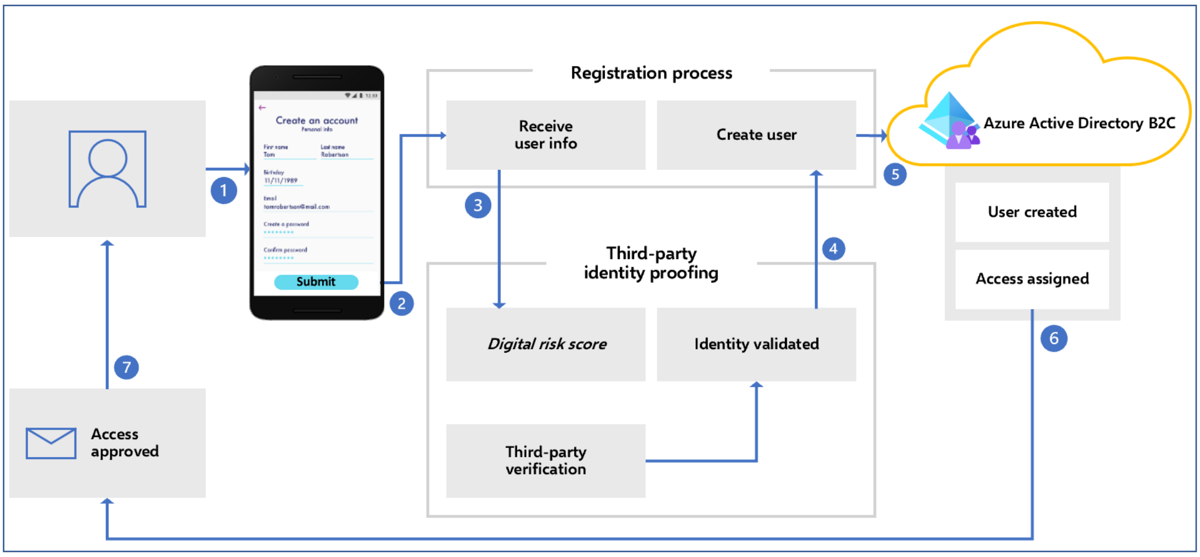
1. **Improved Security:** Azure B2C provides robust security features, including MFA, protecting user accounts from unauthorized access.



2. **Enhanced User Experience:** Customizable user flows and branding ensure a seamless and consistent experience, increasing user satisfaction.



3. **Compliance:** Azure B2C helps organizations adhere to privacy regulations like GDPR by securely managing user data.



4. **Scalability:** The service scales with your app's growth, ensuring that authentication and authorization processes remain performant.
5. **Cost-Efficiency:** While there is a cost associated with Azure B2C, it often proves cost-effective compared to building and maintaining custom authentication systems.

Conclusion

In today's digital landscape, user authentication and authorization are crucial aspects of app development. Azure B2C simplifies this process by offering a comprehensive, customizable, and secure solution. By leveraging Azure B2C, developers can focus on building great user experiences while ensuring the highest level of security and compliance. While there may be challenges in implementing Azure B2C, the business benefits far outweigh them, making it an essential tool in the Microsoft Azure ecosystem for modern app development.

References:

https://learn.microsoft.com/en-us/azure/active-directory-b2c/

pivots=b2c-user-flow

programming-language-csharp

By VIJAYALAXMI

(vijayalaxmibcheruku@gmail.com)