

Visual Studio **LIVE!** | AUSTIN
EXPERT SOLUTIONS FOR ENTERPRISE DEVELOPERS

Modern Authentication and Authorization with OIDC, OAuth2, and Resource-based Permissions

Eric D. Boyd
Founder & CEO
responsiveX

April Rains
Senior Consultant
responsiveX

Azure MVP
Microsoft Regional Director

Level: Intro-Intermediate

#VSLIVE

NO CODE LIMITS



Eric Boyd

✉ eric.boyd@responsiveX.com

🐦 @EricDBoyd



Microsoft
Regional Director



April Rains

✉ april.rains@responsiveX.com

responsiveX

Infrastructure // App Dev // Data and AI // DevSecOps

Visual Studio LIVE!
EXPERT SOLUTIONS FOR ENTERPRISE DEVELOPERS

Identity solution considerations



Identity
Management



Authentication



Authorization



Federation



Delegation



Accounting

Visual Studio LIVE!
EXPERT SOLUTIONS FOR ENTERPRISE DEVELOPERS



Identity Management

What information do we have about a user?

How is this information created, updated and managed?



Authentication (AuthN)

Who do you say you are?

Are you who you say you are?

Can we verify credentials securely?

What telemetry data do we capture and store?





Authorization (AuthZ)

What can you access?

What permissions should you be granted?

Permission and access control enforcement across services and applications.



Federation

Enabling systems and identity providers to use identities from trusted external identity providers





Delegation

Enabling a system or service to act on behalf of the identity of the client or calling system or service



Accounting

Report on, analyze, and monitor the identities and activities across the identity and access control systems

Identity solution considerations



Identity
Management



Authentication



Authorization



Federation

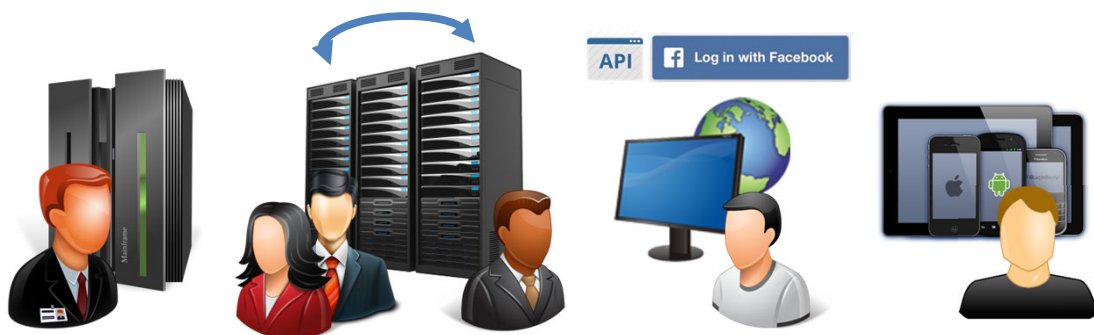


Delegation



Accounting

Evolution of Computing

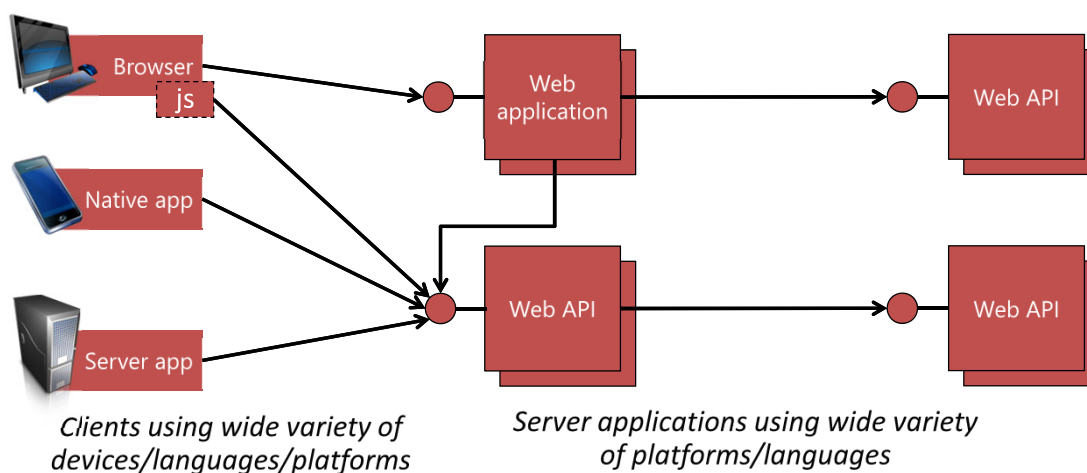


Connected Things



Visual Studio LIVE!
EXPERT SOLUTIONS FOR ENTERPRISE DEVELOPERS

Authentication Scenarios

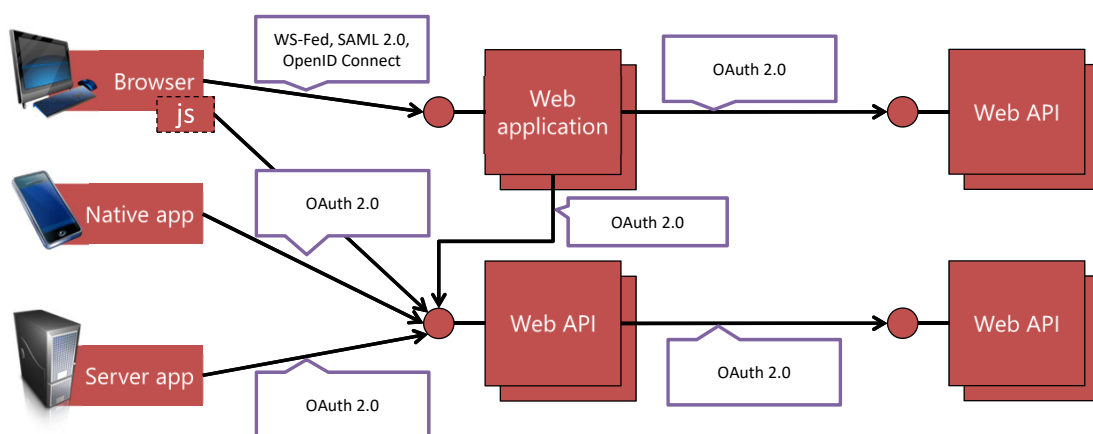


Visual Studio LIVE!
EXPERT SOLUTIONS FOR ENTERPRISE DEVELOPERS

Welcome Claims-based Identity



Authentication Scenarios



Resource owner

Typically, the application user, or end-user.

The end-user "owns" the protected resource your app accesses on their behalf.

The resource owner can grant or deny the client access to the resources they own.



Clients

The application or system that trusts the IdP or authorization server and requests tokens for authenticating users and accessing resources.

Often referred to as relying party or RP.

Examples include web applications, SPAs, mobile apps, desktop apps, and server processes.



Resources

The APIs and identity data you want to protect.

Also referred to as a resource server.



Identity Provider

The *authority* that knows about the actors/users/entities.

Often referred to as IPs, IdPs or authorities.

Examples include Active Directory and Facebook.



Authorization Server

The application server responsible for issuing tokens to clients.

Also referred to as an OpenId Connect provider or security/secure token service (STS).

Sometimes combined with the IdP as a single service.

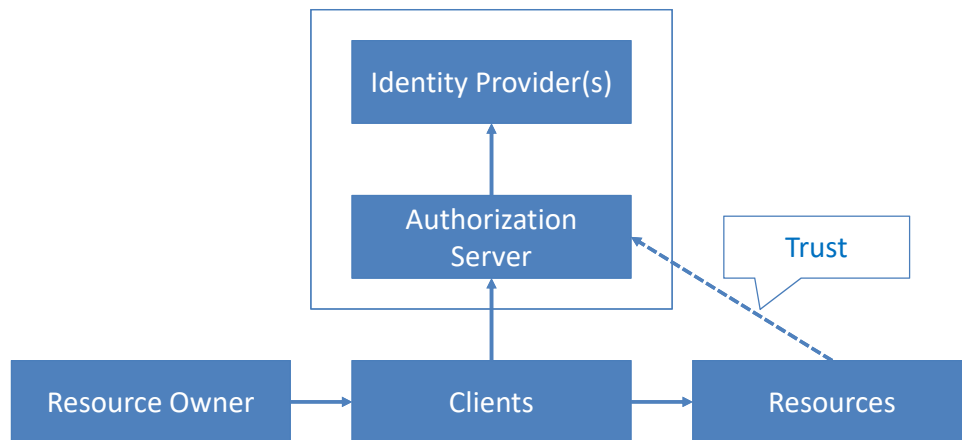


Trust

The client (*relying party*) believes what the IdP or authorization server says about the resource owner or user.



OpenID Connect and OAuth 2.0



Token(s)

Used to identify the IdP from any application, to provide the results of an authentication operation from an IdP, to provide access to API resources.

Identity token (id_token)
Authentication result



Access token
Access to an API resource

Claims

Attributes about a user, serialized into a token, and passed around.



Claims about the user

Usage	Claim Type	Claim Value
 Security	Object ID	b3809430-6c28-4e43-870d-fa7d38636dcd
	Tenant ID	81aabdd2-3682-48fd-9efa-2cb2fcea8557
	Subject	m70fSk8OdeYYyCYy6C3922lmZMz9JKCGR0P1
 Display	Name	frank@contoso.com
	First Name	Frank
	Last Name	Miller

Token format

- Identity tokens
 - Structured
 - JSON Web Tokens (JWT)
- Access tokens
 - Bearer tokens
 - No defined spec or structure
 - Intended to be opaque
 - Self-contained
 - JWTs



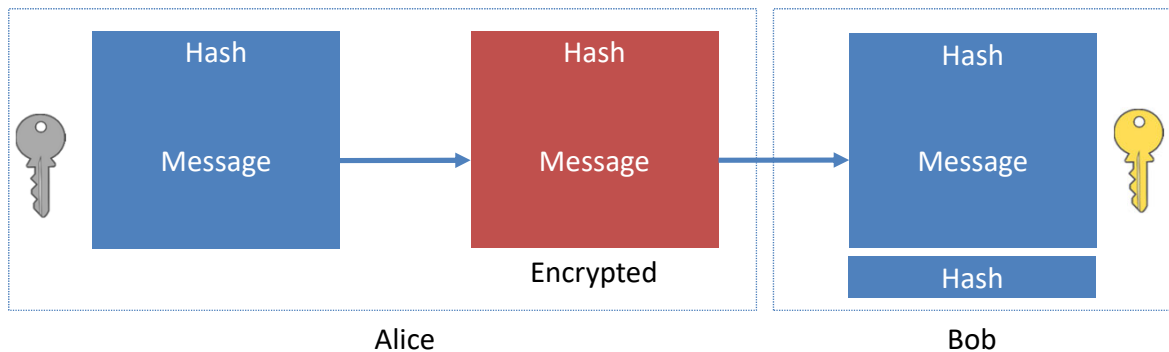
JSON Web Tokens (JWT)

- Three parts
 - Header
 - Payload/Data
 - Signature
- Base64 encoded
- Separated by . (dots)
- JWT Tools
 - <https://jwt.io>
 - <https://jwt.ms>



Digital Signature

Used to ensure a message came from a specific source and hasn't been modified.



Can I use ASP.NET Identity
or ASP.NET Core Identity?

What can I use?

Services like Azure Active Directory, Okta, Auth0, and more.

Products like IdentityServer, Gluu Server, Keycloak, and more.

<https://openid.net/developers/libraries/>

What can I use?

Services like Azure Active Directory, Okta, Auth0, and more.

Products like IdentityServer, Gluu Server, Keycloak, and more.

<https://openid.net/developers/libraries/>

Microsoft Identity Platform

- **OAuth 2.0 and OpenID Connect standard-compliant authentication service**
 - Work or school accounts, provisioned through Azure Active Directory (AAD B2B)
 - Personal Microsoft account, like Skype, Xbox, and Outlook.com
 - Social or local accounts, by using Azure Active Directory B2C (AAD B2C)
- **Open-source libraries**
 - Microsoft Authentication Libraries (MSAL)
 - Support for other standards-compliant libraries
- **Application management portal**
 - A registration and configuration experience in the Azure portal
- **Application configuration APIs**
 - Programmatic configuration of your applications through the Microsoft Graph API
 - PowerShell cmdlets so you can automate your DevOps tasks.

Azure Active Directory

Azure Active Directory Free

User and group management, on-premises directory synchronization, basic reports, self-service password change for cloud users, and single sign-on across Azure, Microsoft 365, and many popular SaaS apps.

Azure Active Directory Premium P1

Also lets hybrid users access both on-premises and cloud resources and supports advanced administration, such as dynamic groups, self-service group management, Microsoft Identity Manager, and cloud write-back capabilities, which allow self-service password reset for your on-premises users.

Azure Active Directory Premium P2

Also offers Azure Active Directory Identity Protection to help provide risk-based Conditional Access to your apps and critical company data and Privileged Identity Management to help discover, restrict, and monitor administrators and their access to resources and to provide just-in-time access when needed.

"Pay as you go" feature licenses

Additional feature licenses, such as Azure Active Directory Business-to-Customer (B2C) to help you provide identity and access management solutions for customer-facing apps.

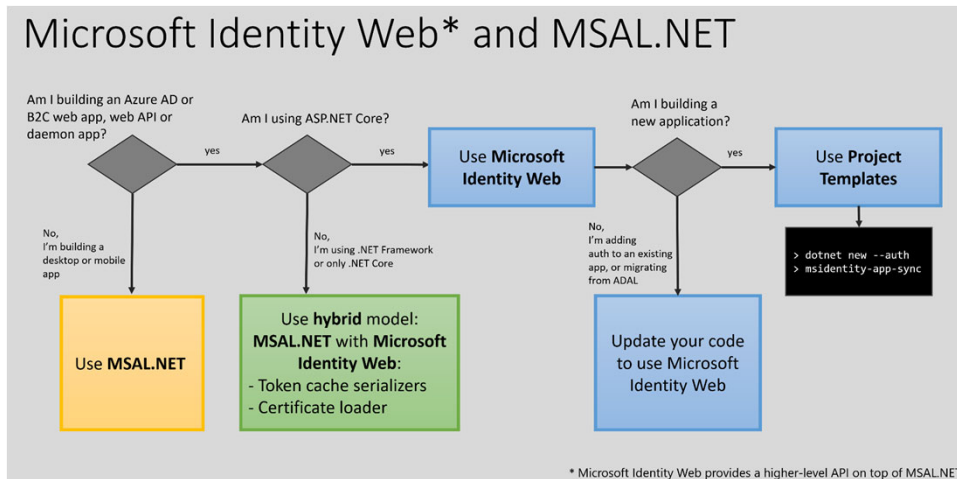
<https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/active-directory-what-is>

Libraries

- Microsoft Authentication Library (MSAL)
 - <https://docs.microsoft.com/en-us/azure/active-directory/develop/msal-overview>
 - <https://docs.microsoft.com/en-us/azure/active-directory/develop/reference-v2-libraries>
- Microsoft.Identity.Web
 - <https://docs.microsoft.com/en-us/azure/active-directory/develop/microsoft-identity-web>



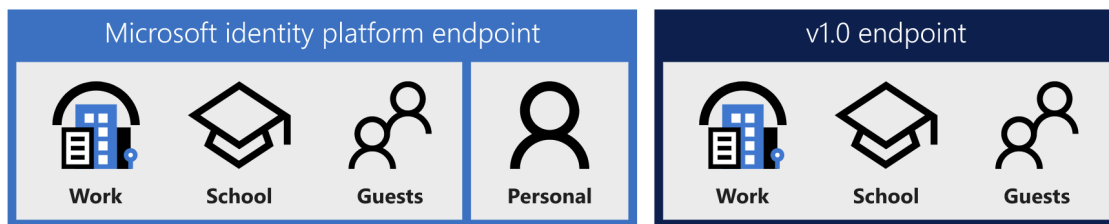
MSAL.NET or Microsoft.Identity.Web?



<https://github.com/AzureAD/microsoft-authentication-library-for-dotnet/wiki/MSAL.NET-or-Microsoft.Identity.Web>

What about ADAL?

- ADAL is the Azure AD Authentication Library
 - Azure AD for developers platform (v1.0)
 - Azure AD identities (work and school accounts)



Visual Studio LIVE!
EXPERT SOLUTIONS FOR ENTERPRISE DEVELOPERS

What about ADAL?

- **June 30th, 2020**, no new features will be added to ADAL and Azure AD Graph
- **June 30th, 2022**, support for ADAL and Azure AD Graph ends. No technical support or security updates.
- Compare MSAL (v2) and ADAL (v1)
 - <https://docs.microsoft.com/en-us/azure/active-directory/azuread-dev/azure-ad-endpoint-comparison>
 - <https://docs.microsoft.com/en-us/azure/active-directory/develop/msal-net-differences-adal-net>

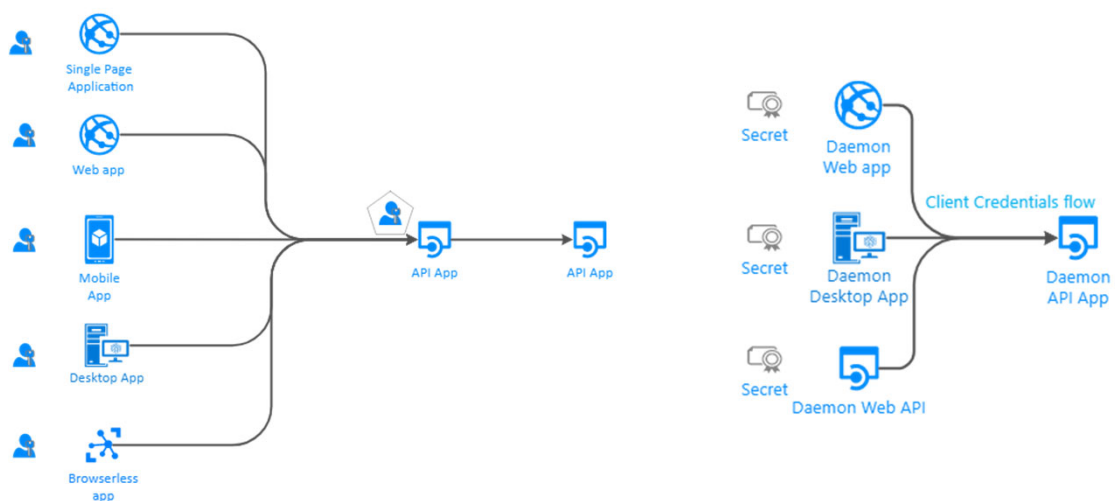
Visual Studio LIVE!
EXPERT SOLUTIONS FOR ENTERPRISE DEVELOPERS

DEMO

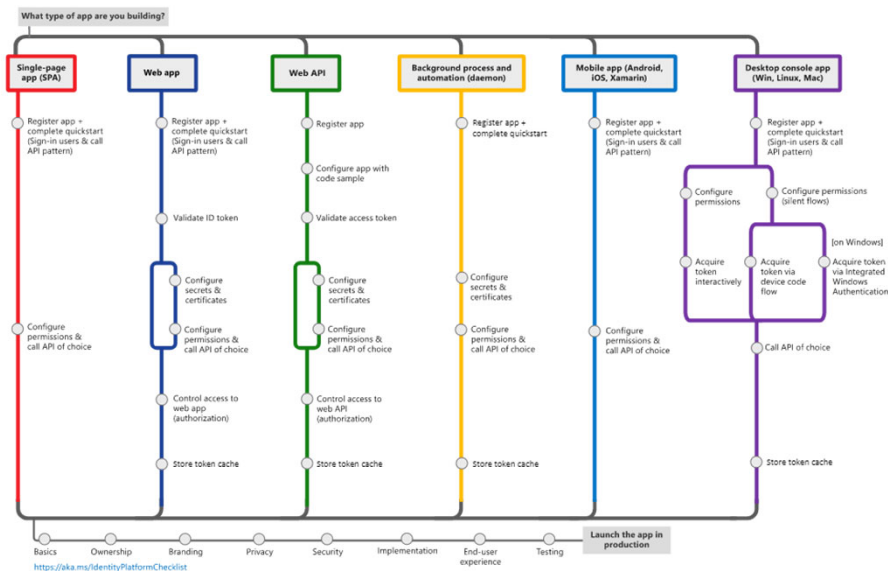
MICROSOFT IDENTITY PLATFORM & AZURE ACTIVE DIRECTORY

Visual Studio **LIVE!**
EXPERT SOLUTIONS FOR ENTERPRISE DEVELOPERS

Authentication Flows



Identity Scenarios Metro Map



Authorization

- Role-based
 - The function applied to the user/identity that implies a set of responsibilities and permissions
- Claims-based
 - Using attributes about the user/identity for authorization decisions
- Resource-based
 - Attributes about the user/identity, combined with attributes about the resource, to make authorization decisions
- Policy-based
 - Authorization rules using a one or more role, claims, and resource-based authorization rules, packaged in a named, reusable module

DEMO

AUTHORIZATION



Duende IdentityServer

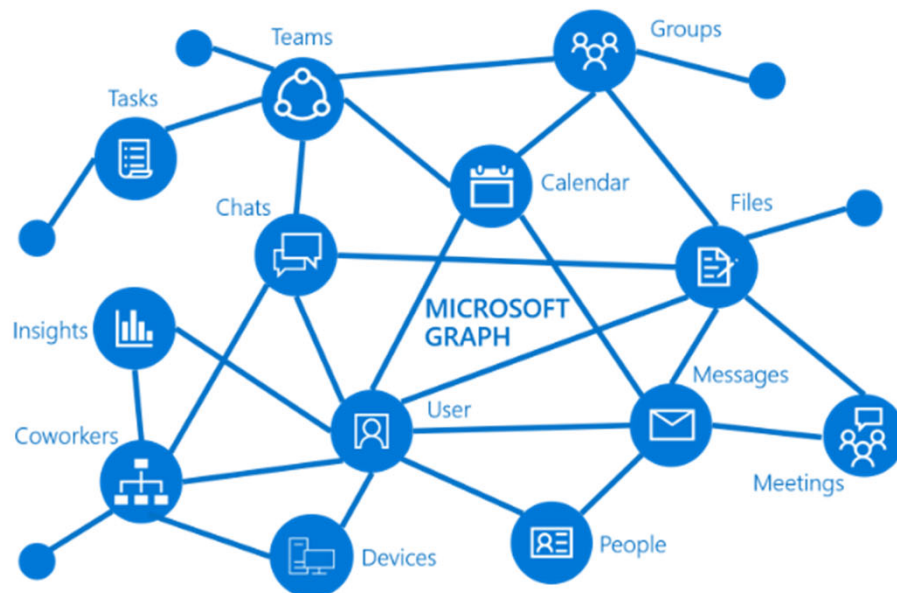
- Standards compliant and flexible OIDC and OAuth2 framework
 - Full control over hosting
 - Full control over UI, UX, business logic, and data
- IdentityServer 4 and earlier
 - Open-source and free
 - .NET Framework and .NET Core
 - Supported until November 2022
- Duende IdentityServer
 - Open-source with a commercial license
 - .NET Core



DEMO

IDENTITYSERVER

Visual Studio **LIVE!**
EXPERT SOLUTIONS FOR ENTERPRISE DEVELOPERS



DEMO

MICROSOFT GRAPH API

Resources

- ASP.NET Identity
 - <https://docs.microsoft.com/en-us/aspnet/core/security/>
- Microsoft Identity Platform
 - <https://docs.microsoft.com/en-us/azure/active-directory/develop/>
- Microsoft Graph
 - <https://docs.microsoft.com/en-us/graph/overview>
- IdentityServer
 - <https://duendesoftware.com/products/identityserver>

Questions



Questions?



Eric Boyd

✉ eric.boyd@responsiveX.com

🐦 [@EricDBoyd](https://twitter.com/EricDBoyd)



April Rains

✉ april.rains@responsiveX.com



Session Survey

- Your feedback is very important to us
- Please take a moment to complete the session survey found in the mobile app
- Use the QR code or search for “Converge360 Events” in your app store
- Find this session on the Agenda tab
- Click “Session Evaluation”
- Thank you!

