April 18th-20th, 2024

#GlobalAzure


Nash Tech.
BY COMMUNITY • FOR COMMUNITY
IN VIETNAM
#GLOBALAZURE
2024
organized by
DEV CAFE
Connect and share
20th April, 2024

DEV Cafe

@DEVCafeVn · 1.19K subscribers · 31 videos

Được bảo trợ bởi NashTech, DEV Cafe là một sân chơi dành cho các anh em lập trình viên t...

facebook.com/devcafevn and 1 more link

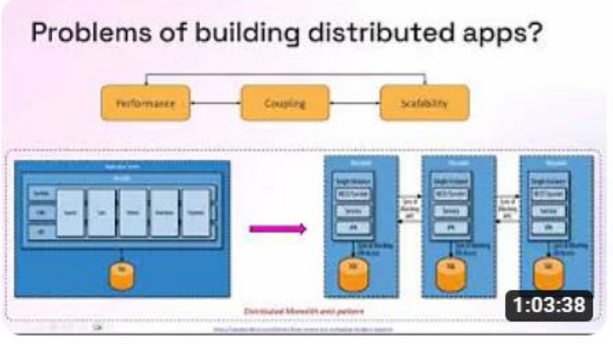
Subscribed

Home Videos Playlists Community

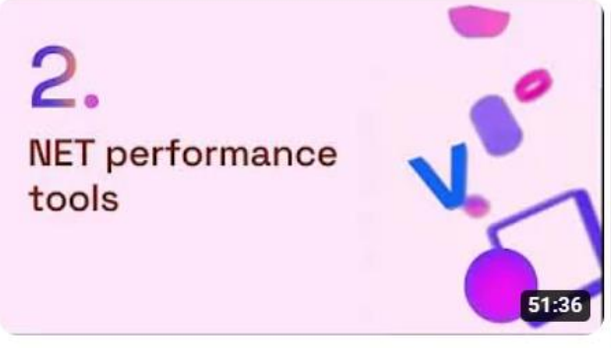
For You

[Vietnamese] Yas - Introduction

2.1K views • 3 months ago



[Vietnamese] Building Portable Event-Driven .NET 8 Apps with Dapr and Radius - Thang Chung



[Vietnamese] High performance programming in .NET - Hai Nguyen

[Vietnamese] Blazor vs JavaScrip Frameworks - Thien Nguyen

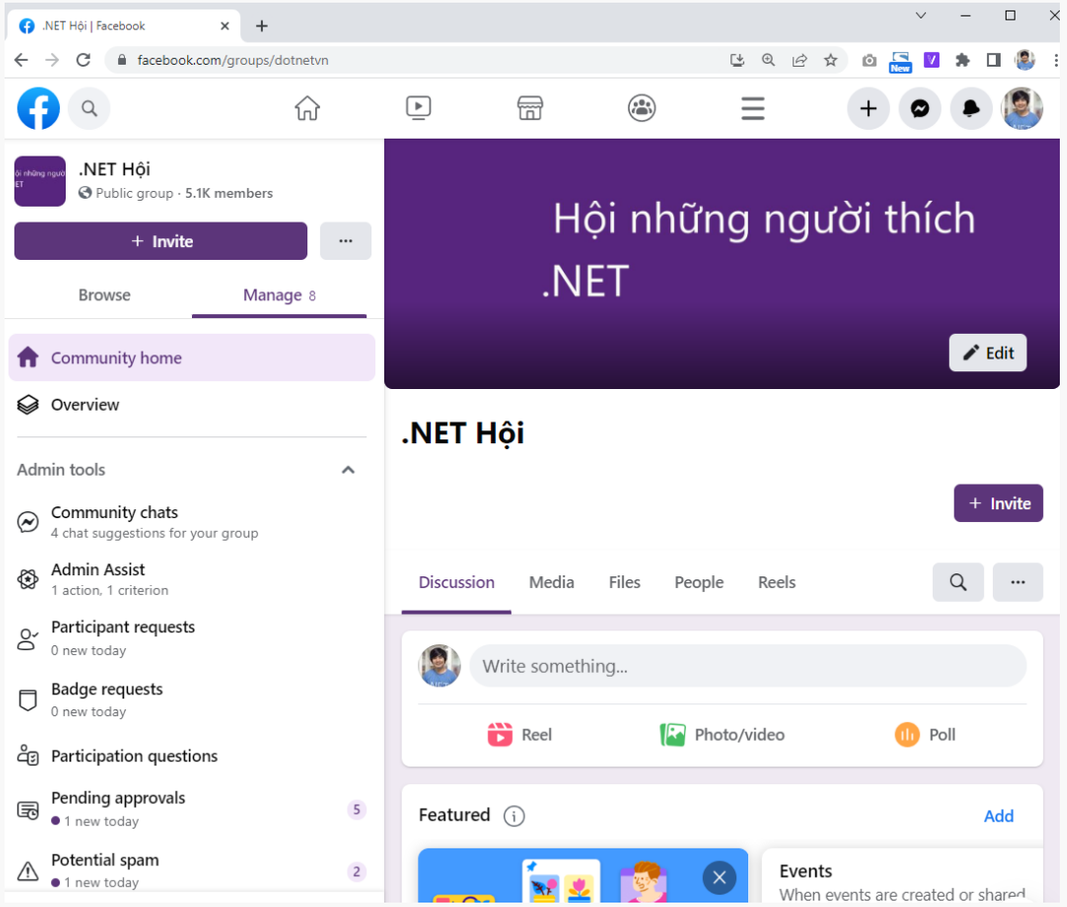
#Vietnam

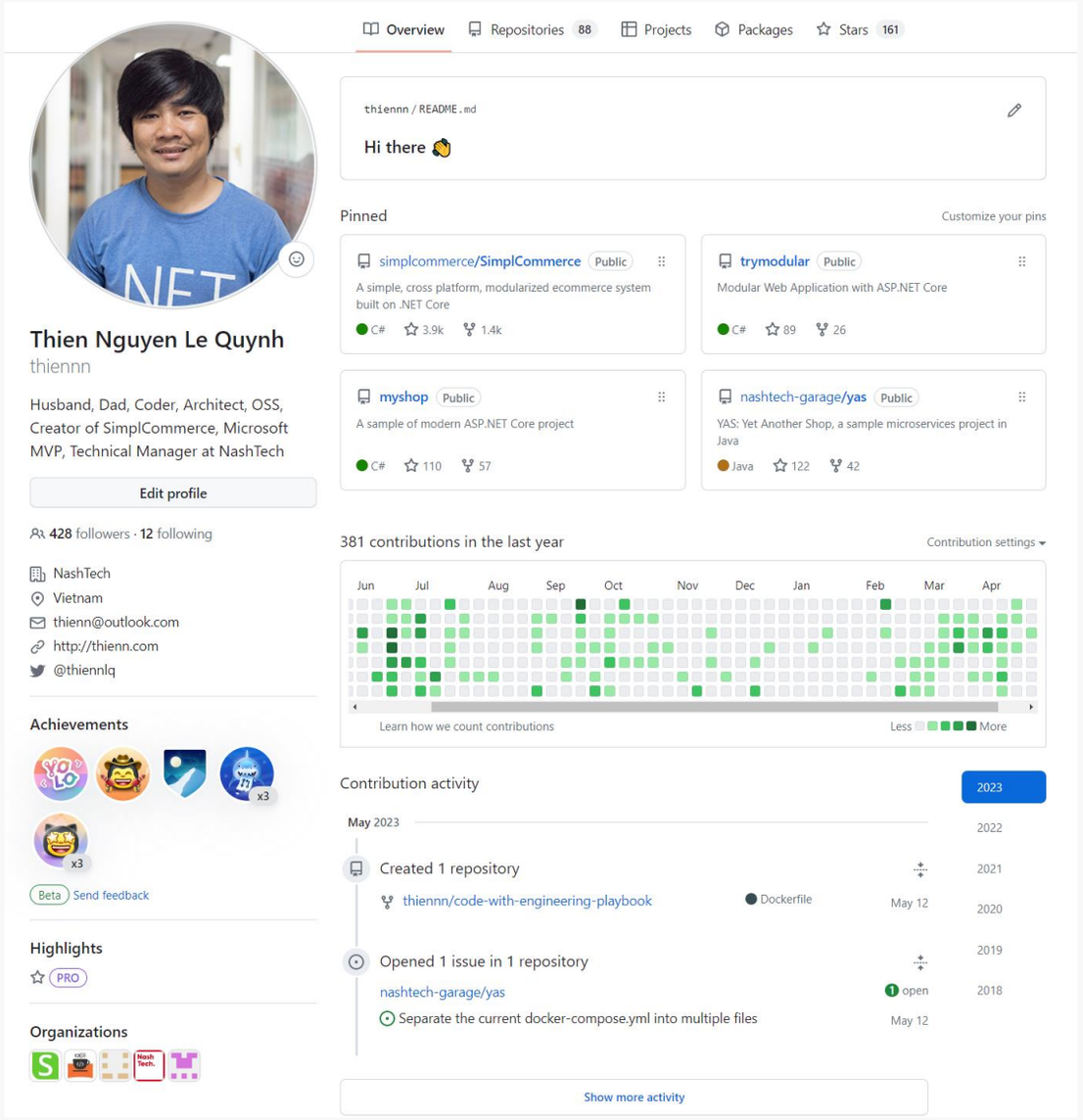
Microsoft Entra ID for developers

Thien Nguyen

About me

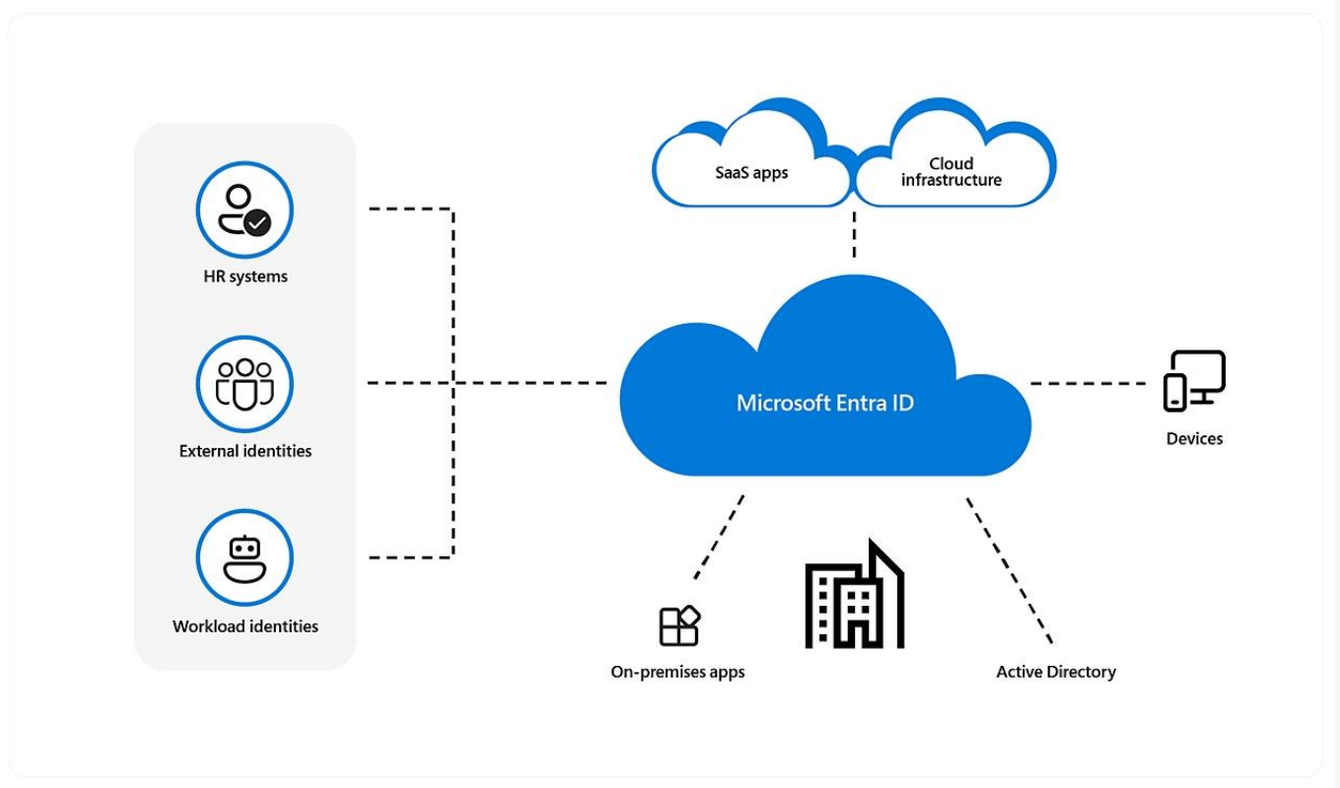
https://www.facebook.com/groups/dotnetvn
https://github.com/thiennn



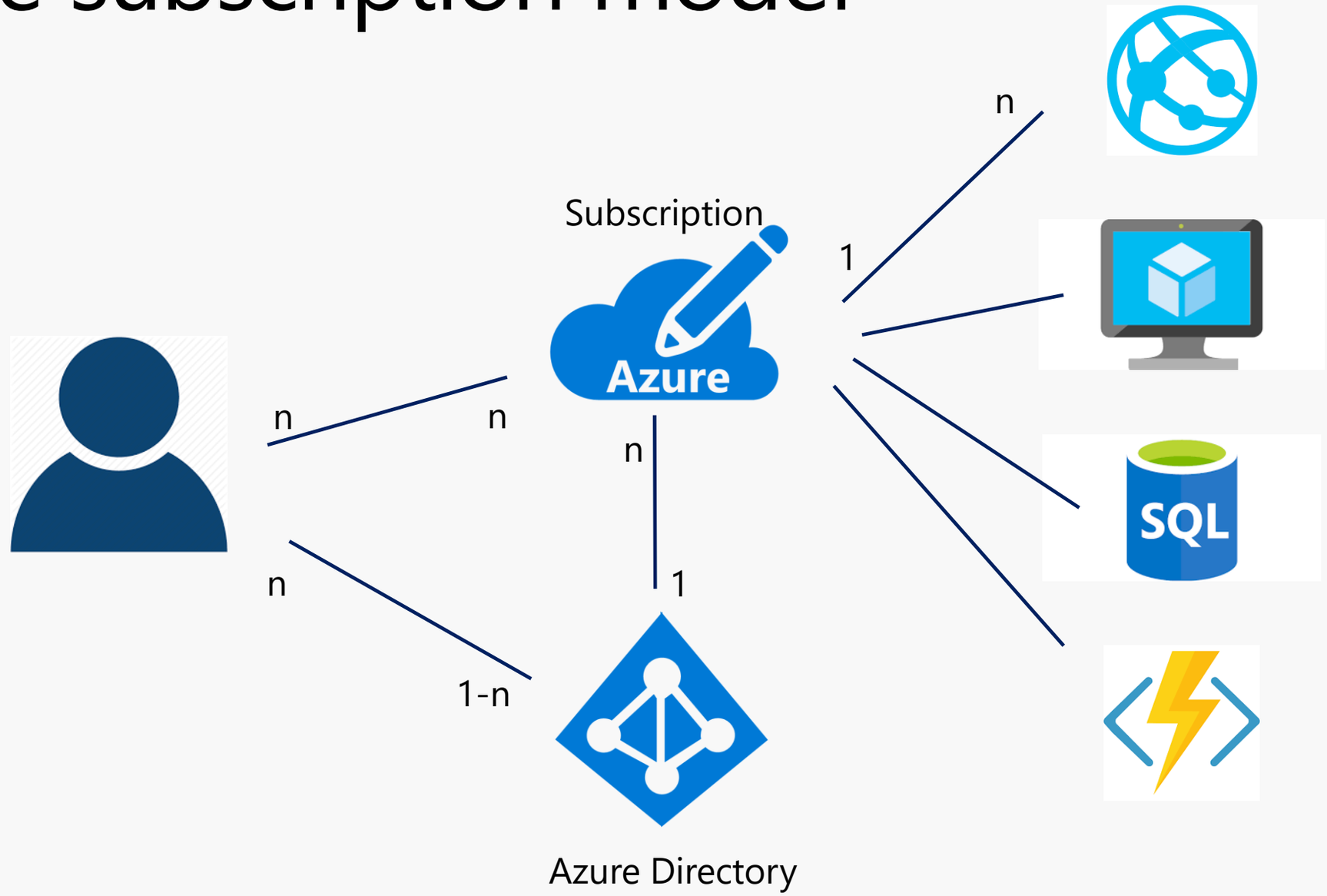


Microsoft Entra ID

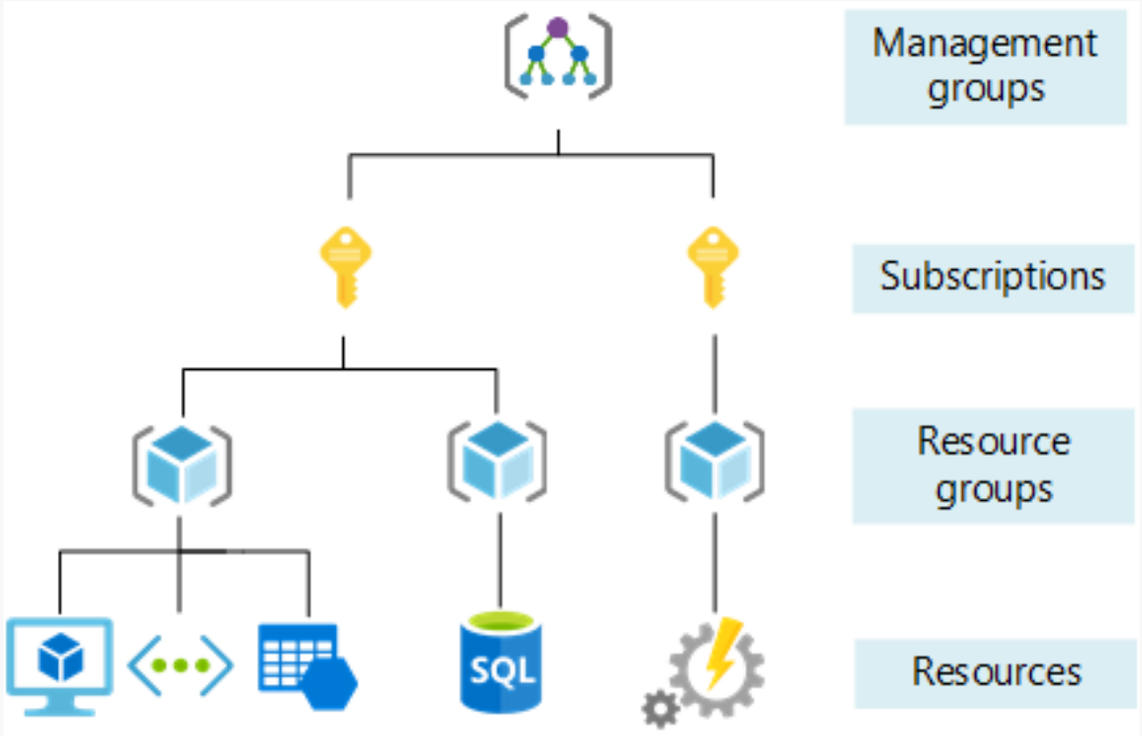
- Microsoft Entra is the name for the product family of identity and network access solutions including Entra ID, Entra Verified ID, Entra Permissions Management, Entra Workload ID,…
- Microsoft Entra ID is a cloud-based identity and access management service that your employees can use to access external resources. Example resources include Microsoft 365, the Azure portal, and thousands of other SaaS applications.



Azure subscription model



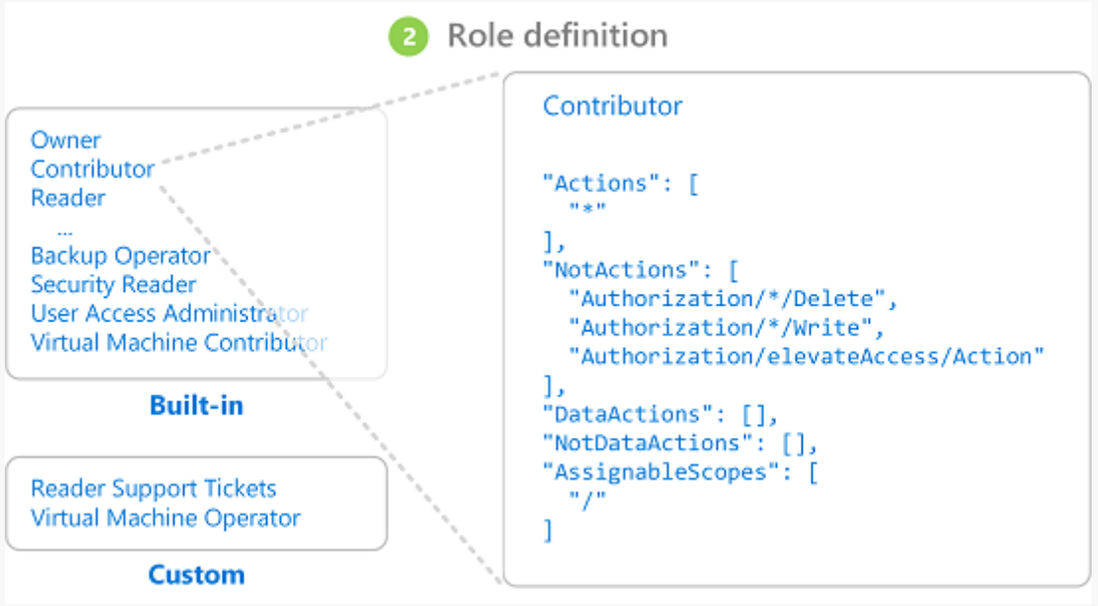
Azure management levels and hierarchy

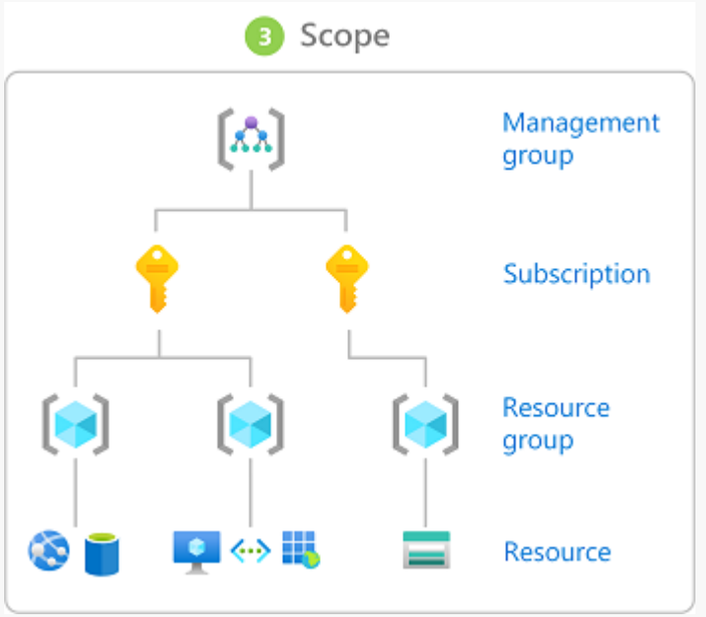


- **Management groups** help you manage access, policy, and compliance for multiple subscriptions. All subscriptions in a management group automatically inherit the conditions that are applied to the management group.
- **Subscriptions** Organizations can use subscriptions to manage costs and the resources that are created by users, teams, and projects. Each subscription has limits or quotas on the amount of resources that it can create and use
- **Resource groups** are logical containers where you can deploy and manage Azure resources like web apps, databases, and storage accounts.
- **Resources** are instances of services that you can create, such as virtual machines, storage, and SQL databases

Azure RBAC

A *security principal* is an object that represents a user, group, service principal, or managed identity that is requesting access to Azure resources. You can assign a role to any of these security principals





Lower levels inherit role permissions from higher levels

#Vietnam

SSO with Microsoft Entra ID

OAuth 2.0/OpenID Connect

- OAuth 2.0 which stands for “Open Authorization”, is an authorization framework that enables a third-party application to obtain limited access to an HTTP service

- OpenID Connect (OIDC) is an identity layer built on top of the OAuth 2.0 framework. It allows third-party applications to verify the identity of the end-user and to obtain basic user profile information

The four roles defined by OAuth

- **Resource owner:** Entity that can grant access to a protected resource. Typically, this is the end-user
- **Client**: An application making protected resource requests on behalf of the resource owner
- **Resource server**: Server hosting the protected resources. This is the API you want to access
- **Authorization Server**: Server that authenticates the Resource Owner and issues access tokens after getting proper authorization; Entra ID, Identity Server4, Keycloak, Auth0,…

JWT

- JSON Web Tokens are an open, industry standard RFC 7519 method for representing claims securely between two parties.

- JWTs have three important components.
  - Header: Define token type and the signing algorithm involved in this space.
  - Payload: Define the token issuer, the expiration of the token, and more in this section.
  - Signature: Verify that the message hasn't changed in transit with a secure signature.

<base64-encoded header>.<base64-encoded payload>.<base64-encoded signature>

Token types

- **Access token**: Access token allows a client application to access a specific resource to perform specific actions on behalf of the user. Access tokens are used as bearer tokens means that the bearer (who holds the access token) can access authorized resources without further identification. "cấp quyền truy cập cho người mang cái này". It’s usually a JWT

- **Refresh token**: This is a long-lived token and is used to request a new access token

- **ID token**: The ID token represents as JWT. It was introduced by OpenID Connect (OIDC) to proves that a user has been authenticated and provide information about the user. We cannot use the ID token to call APIs

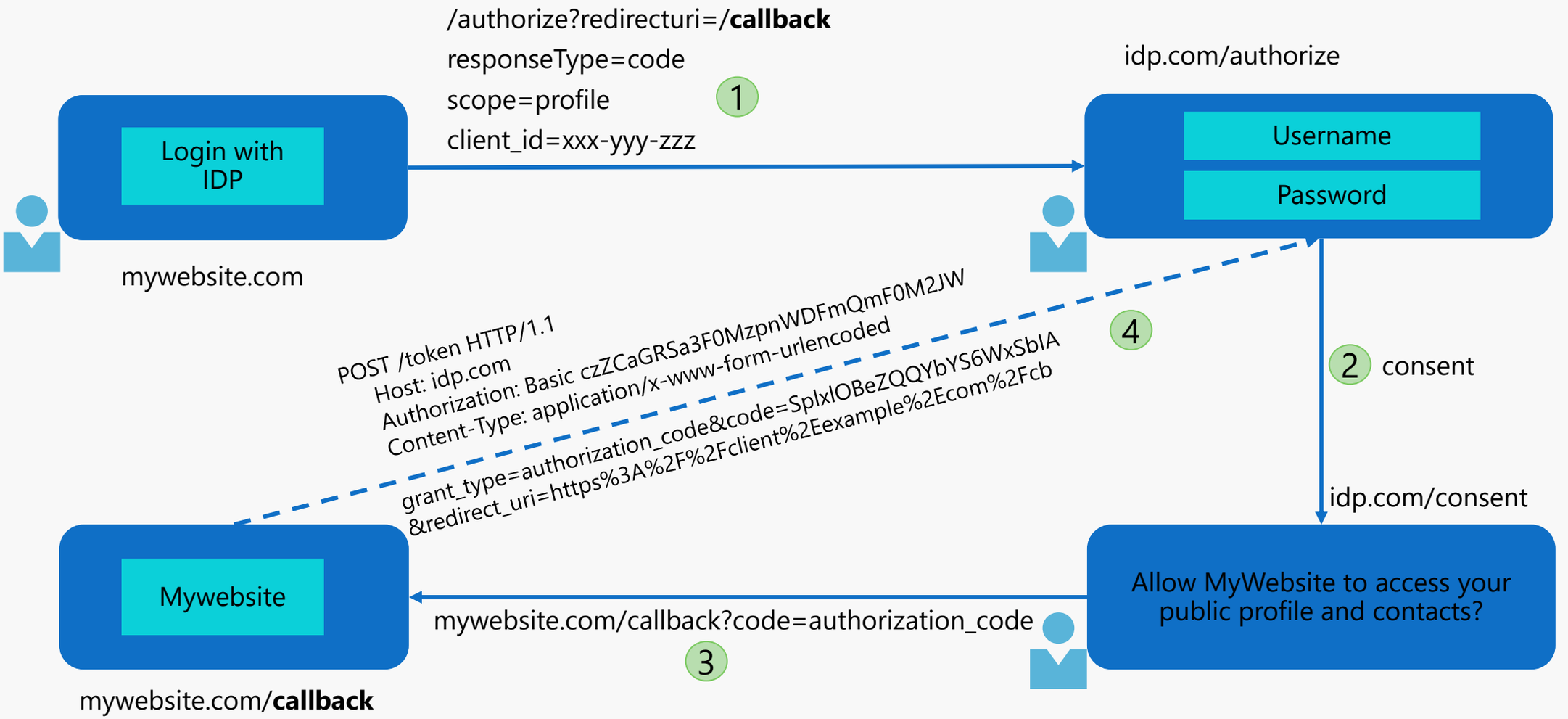
- **Opaque token** (Reference token): An opaque or a reference token is a random and a unique string of characters which has been issued by the token service as an identifier to be used for API authentication purposes. These tokens does not carry any information related to user; hence it is required to open a back channel to the token validation service to validate it and retrieve token information.

Grant Types in OAuth 2.0

Grants are the set of steps a Client must perform to get access token

- Authorization code
- Implicit → Authorization code + PKCE
- Resource owner password (Resource owner credential)
- Client credential

Authorization code



Authorization Code Flow + PKCE

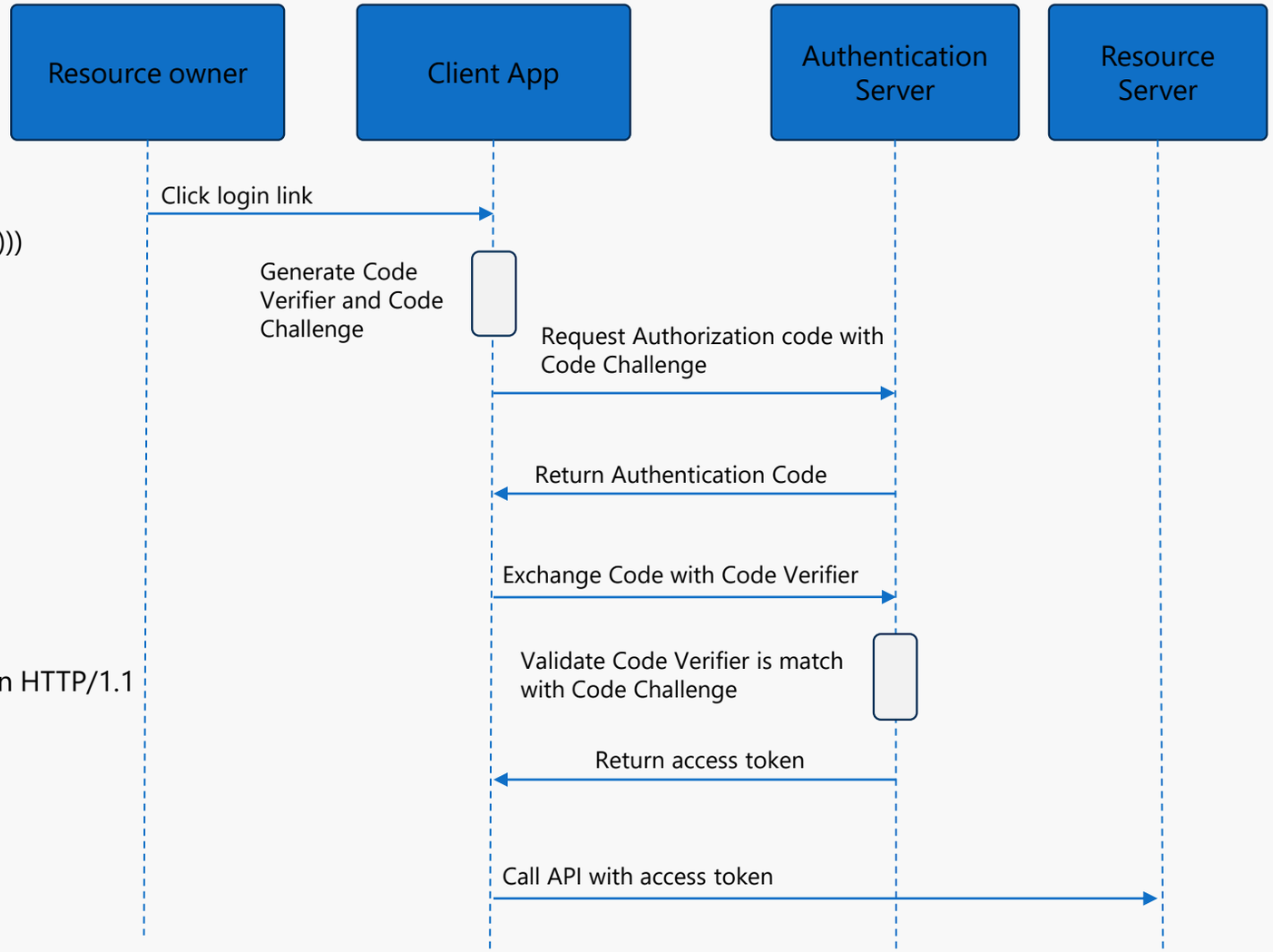
PKCE stands for Proof Key for Code Exchange

code_verifier = random STRING (length 43-128)
code_challenge = BASE64URL-ENCODE(SHA256(ASCII(code_verifier)))

/authorize?redirecturi=/**callback**
&responseType=code
&scope=profile
&client_id=[client_id]
&code_challenge=[code_challenge]
&code_challenge_method=S256

POST http://identity/auth/realms/Yas/protocol/openid-connect/token HTTP/1.1
Host: identity

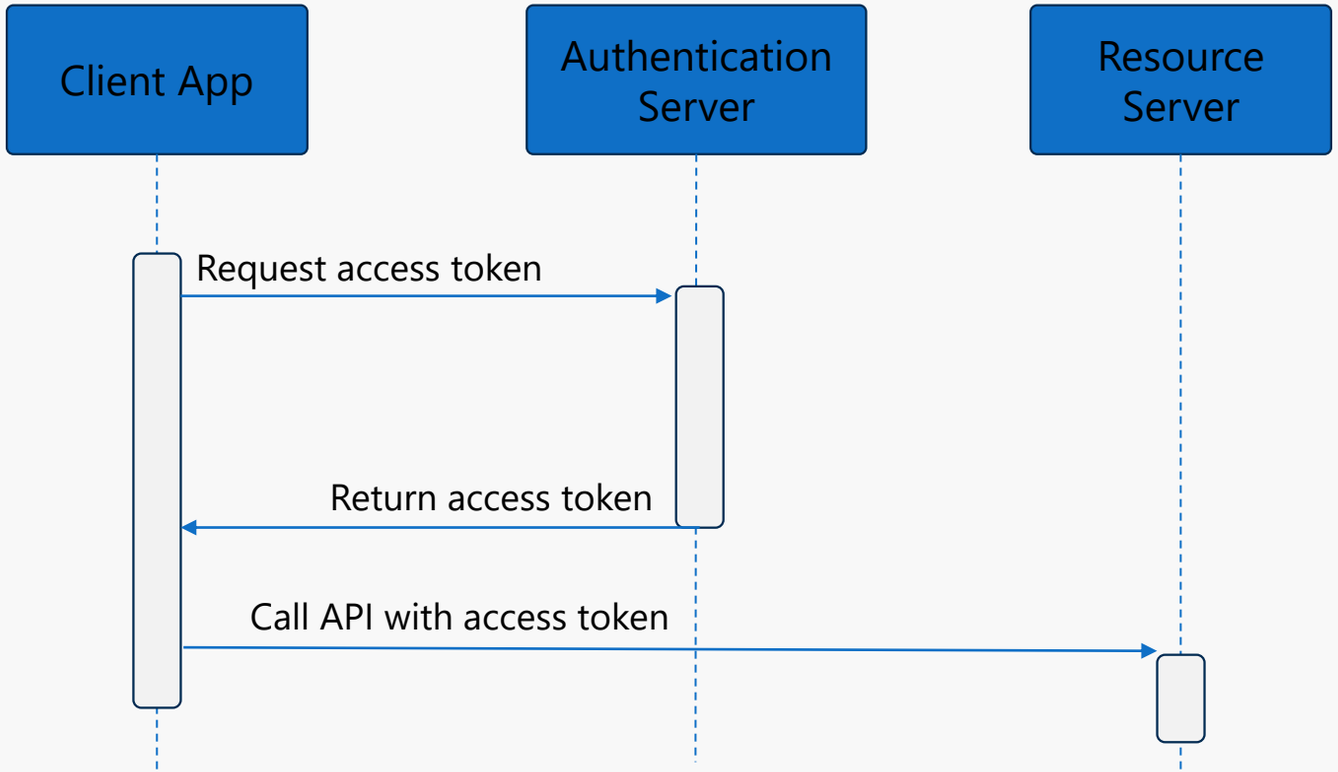
grant_type=authorization_code
&code=[code]
&client_id=[client_id]
&code_verifier=[code_verifier]



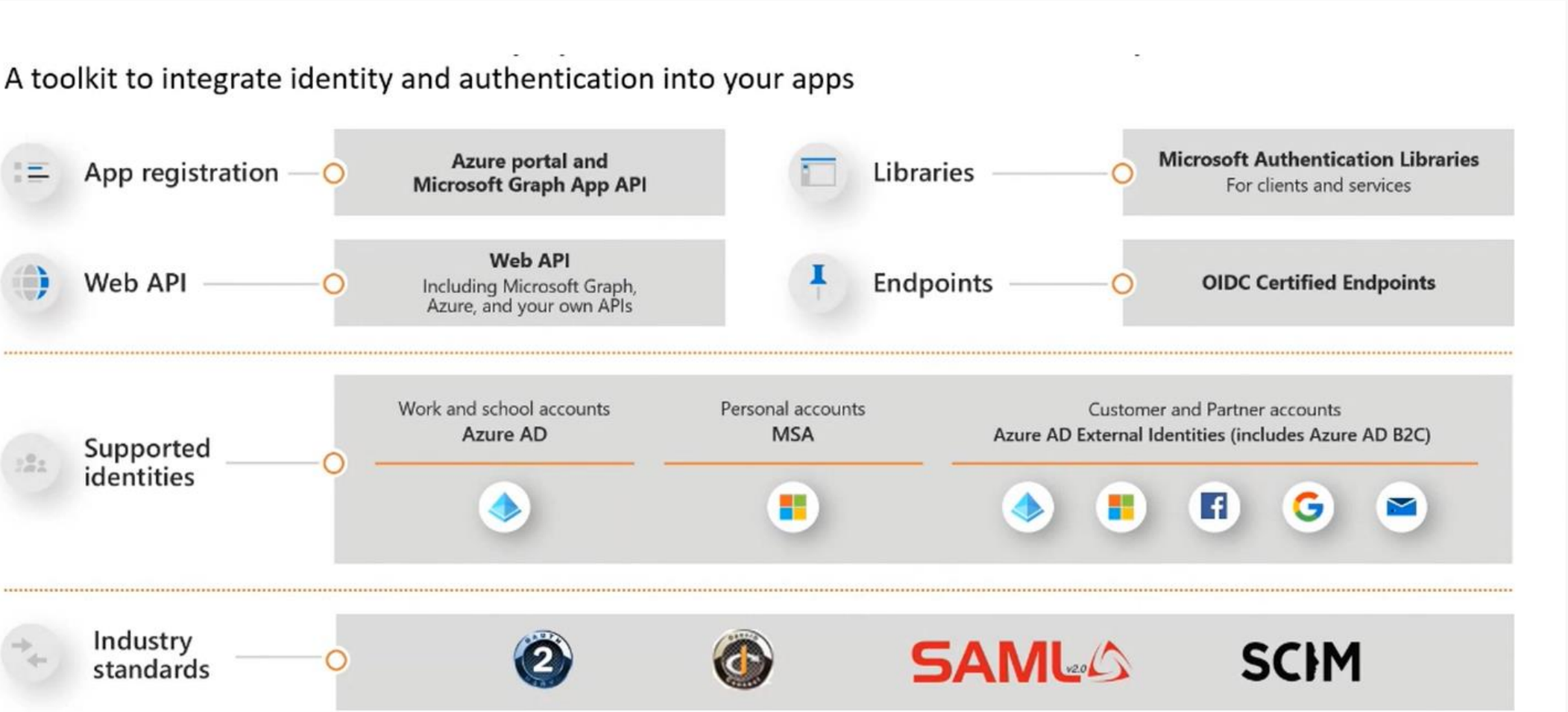
Client credentials

Authorization: Basic <base64 encoded client_id:client_secret>

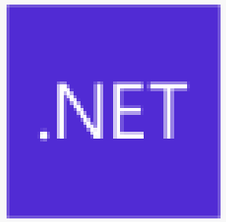
```
POST /token HTTP/1.1
    Host: server.example.com
    Authorization: Basic
czZCaGRSa3F0MzpnWDFmQmF0M2JW
    Content-Type: application/x-www-form-urlencoded

    grant_type=client_credentials
```



Microsoft Identity Platform

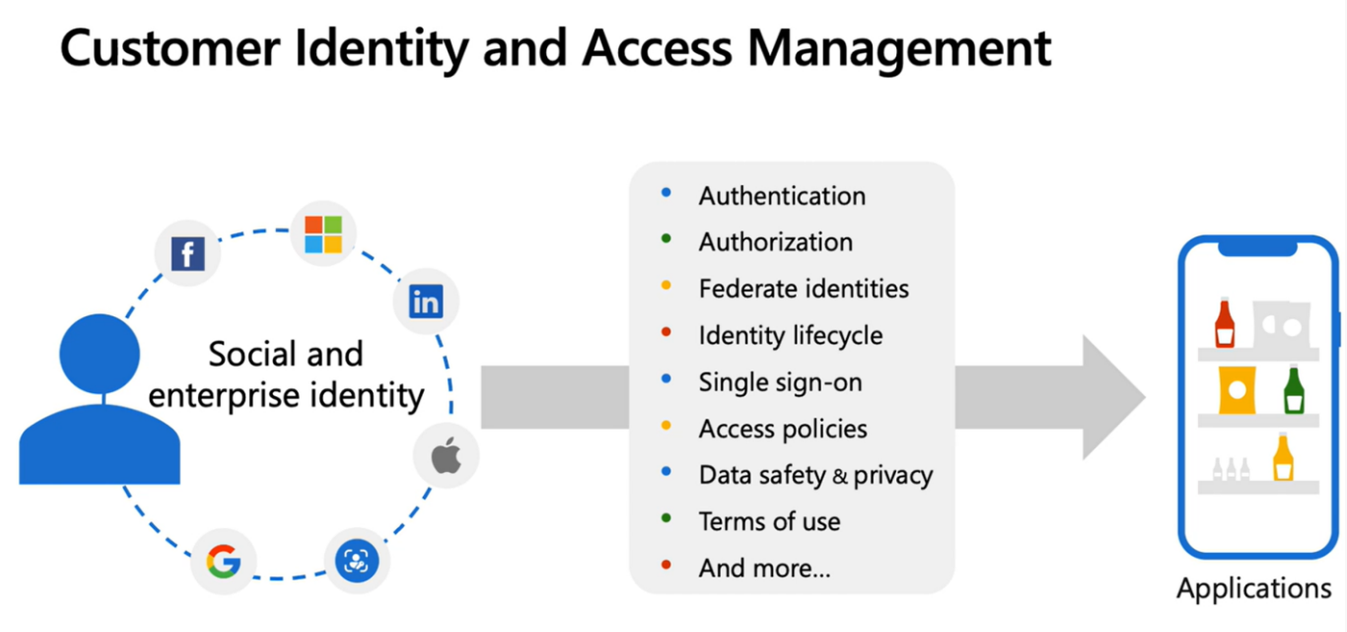


Microsoft Authentication Libraries (MSAL)



https://learn.microsoft.com/en-us/entra/msal/

Microsoft Entra External vs Azure AD B2C



- **Microsoft Entra External ID** is a next-generation customer identity and access management (CIAM) solution for managing all external identities. These include customers, citizens, patients, partners, suppliers, and contractors within a single, unified platform (***in preview***)

- **Azure AD B2C** is our current generation customer identity and access management product. Azure AD B2C will continue to remain a fully supported customer solution. There are no requirements for customers to migrate at this time and no plans to discontinue our current B2C product

Resources

- https://aka.ms/lets-get-technical-oauth
- https://learn.microsoft.com/en-us/entra/identity-platform/v2-overview
- https://dev.azure.com/thienn/SimplAds
- https://datatracker.ietf.org/doc/html/rfc6749
- https://openid.net/specs/openid-connect-core-1_0.html

Thanks for joining !

DEV CAFE
Connect and share

https://www.facebook.com/devcafevn
https://www.youtube.com/c/devcafevn