Application Security
App Security

Hello!

I am Eng Teong Cheah

Microsoft MVP

App Security

Microsoft Identity Platform

◎ OAuth 2.0 and OpenID Connect standard-compliant authentication service

◎ Open-source libraries

◎ Application management portal

◎ Application configuration API and PowerShell

◎ Developer content

Azure AD Application Scenarios

◎ Single page frontends run in a browser

◎ Web browser to a web application

◎ Web API on behalf of a user

◎ Web applications that need resources from a web API

◎ Daemon or server application that needs resources from a web API
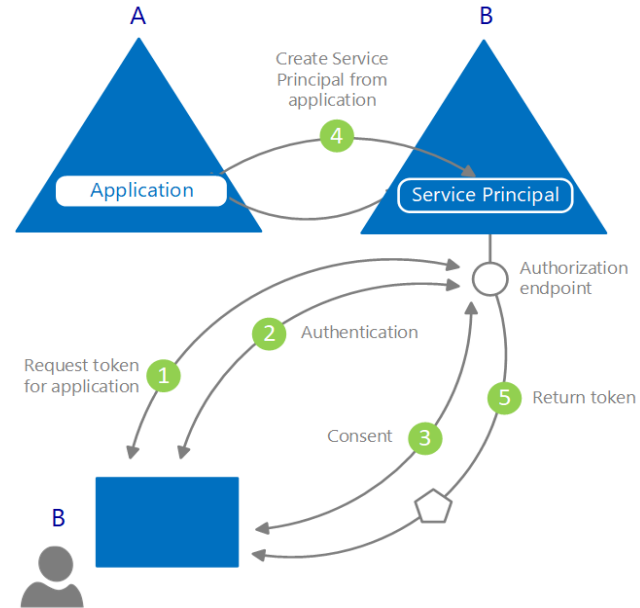
App Registration

◎ Any application that outsources authentication to Azure AD must be registered in a directory

◎ Registration creates token information including a unique application id, one or more endpoints, and an application secret

Microsoft Graph Permissions

◎ Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process

◎ Delegated permissions are used by apps that have a signed-in user present

◎ Application permissions are used by apps that run without a signed-in user present

Web App Certificates

- ◎ Enable require incoming certificate
- ◎ Basic app plan tier or above
- ◎ Requires HTTPs
- ◎ Private or public certificates
- ◎ Allow anonymous access with an exclusion path

Thanks!

Any questions?

You can find me at:

@walkercet

References

◎ https://docs.microsoft.com/en-us/