Microsoft

API Authentication with OAuth2 using Azure AD



Maulik Soni
Sr. Cloud Solutions Architect
Microsoft

https://www.linkedin.com/in/mauliks/

SPEAKER BIO

Key Terms

OAuth 2.0

- Industry protocol for Authorization
- Grants limited access to protected resource
- OIDC is authentication and authorization layer built on top of OAuth2

Tokens

- Lightweight security token that grants “bearer” access to protected resources
- Generally represented as JWT (JSON Web Token)

Azure AD

- Is an Identity Provider (IdP)
- Ensures the user's identity, granting and revoking access to resources, and issuing tokens

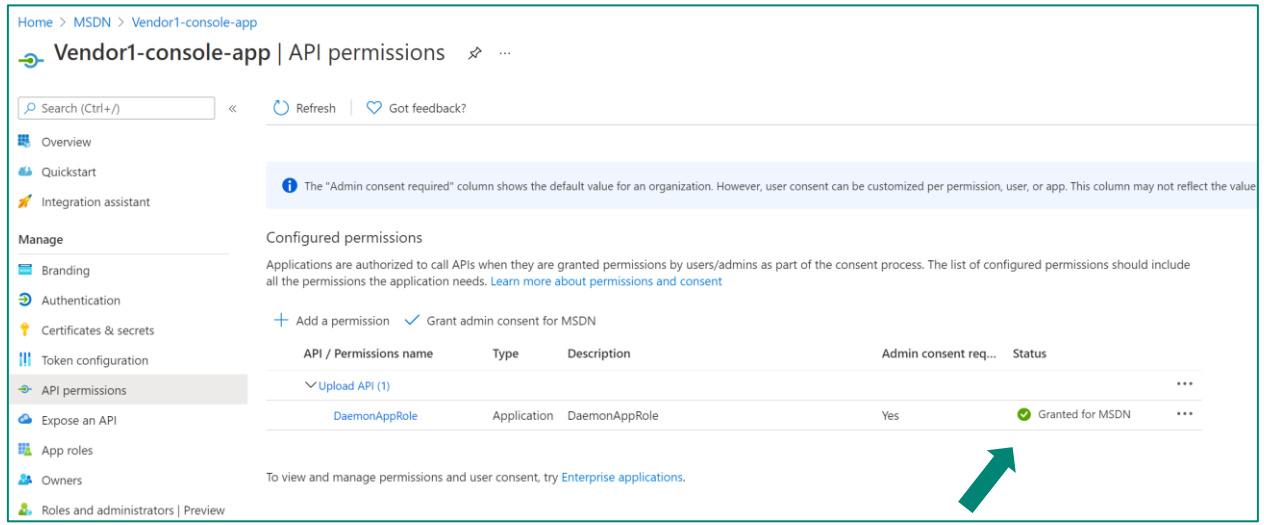
App Registrations & Flows

- Provide authentication and authorization services for your application and its users
- Client Credential Flow - permits a web service (confidential client) to use its own credentials, instead of impersonating a user

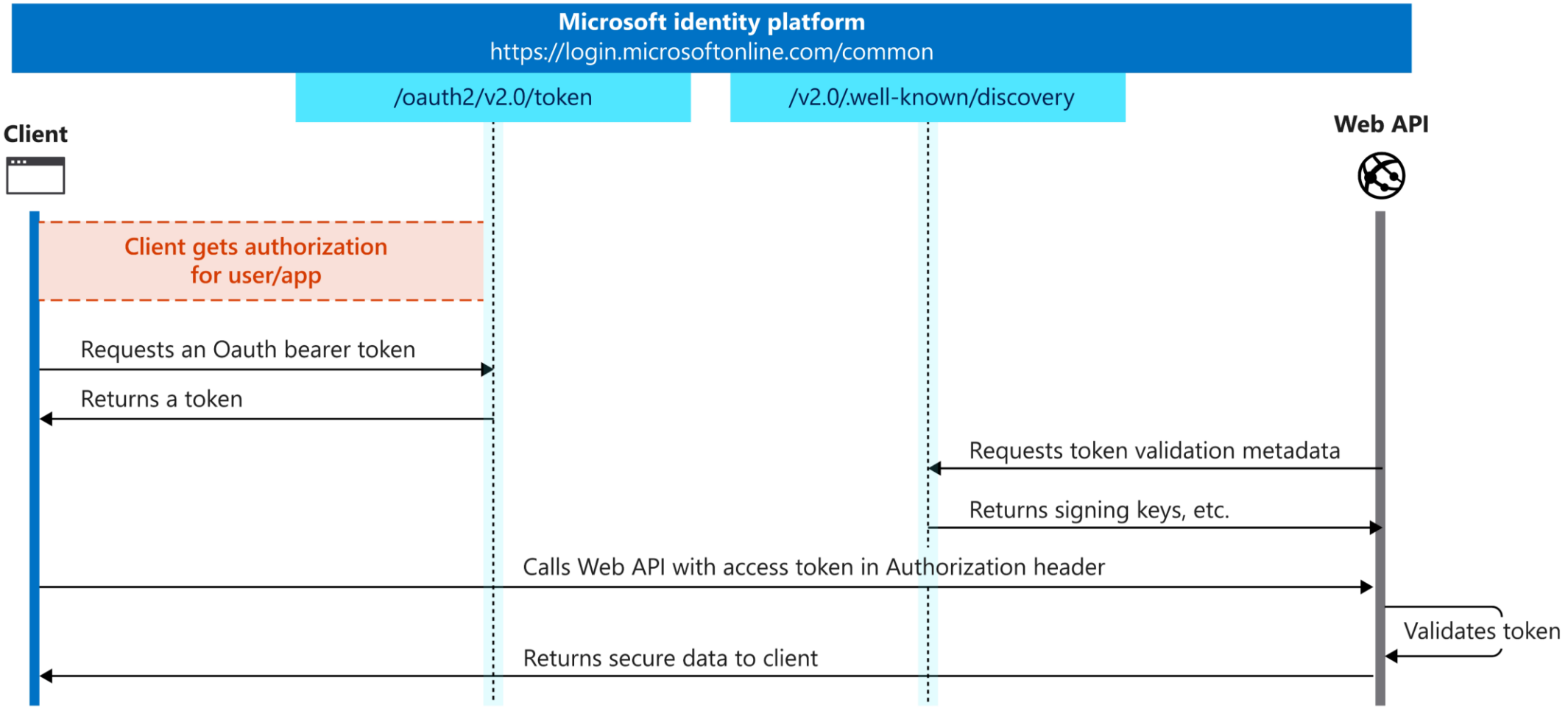
Key Terms

Azure AD Admin Consent

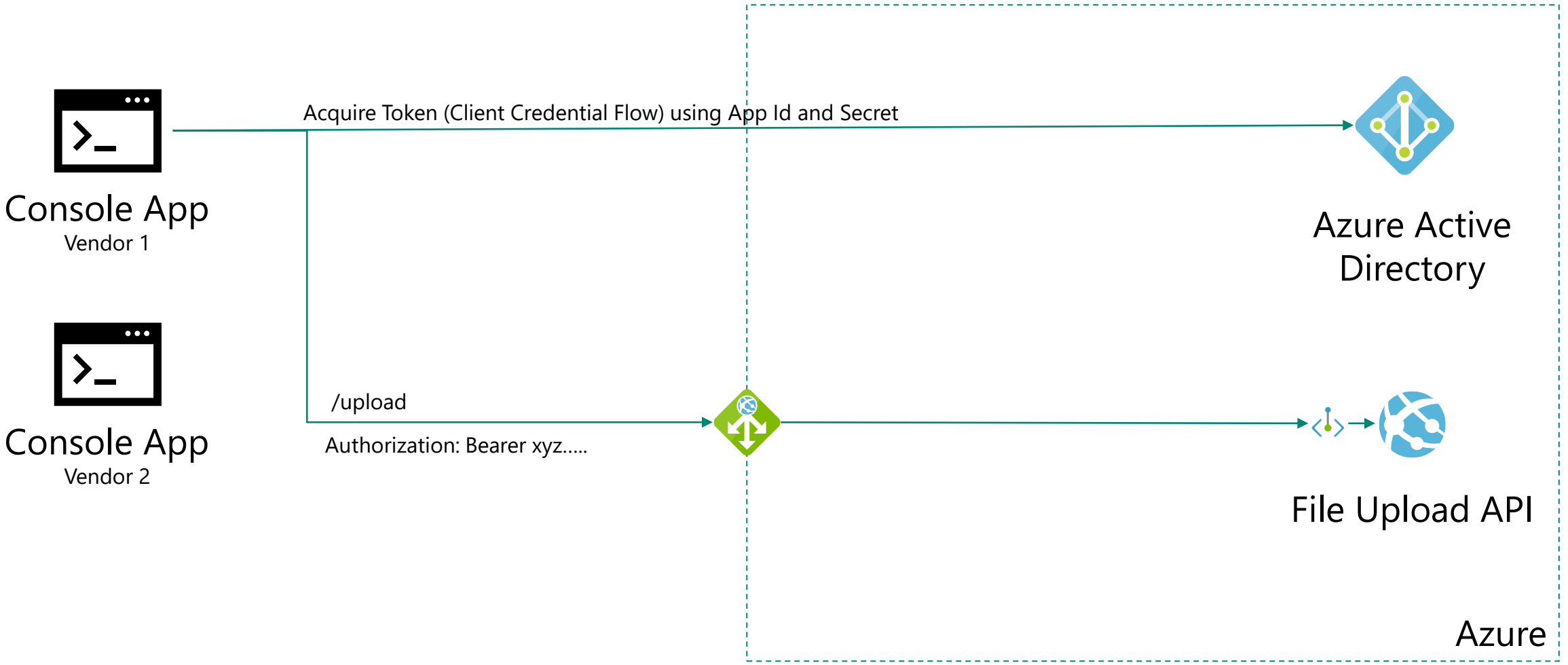
- Application Owner can grant the consent
- Global Admins can grant tenant wide permission.



Authentication Flow



Scenario – Expose file upload API to multiple vendors



Demo

- Register an AAD Application representing a Resource (api)
- Register an AAD Application representing a Client (console app)
  - Generate Client Secret
- Admin Consent Process
- Request a Token
- Validate a Token (Java / C#)
  - https://github.com/mauliksoni/aad-token-validation
- Revoke Client Access

Resources

Microsoft Docs

- OAUTH 2.0 authentication with Azure Active Directory | Microsoft Docs
- OAuth 2.0 and OpenID Connect protocols on the Microsoft identity platform - Microsoft identity platform | Microsoft Docs
- OAuth 2.0 client credentials flow on the Microsoft identity platform | Microsoft Docs
- Application types for the Microsoft identity platform | Microsoft Docs
- Quickstart: Register an app in the Microsoft identity platform | Microsoft Docs
- Microsoft identity platform scopes, permissions, & consent | Microsoft Docs

Self service Role Assignment

Graph Explorer

- Demo

Microsoft

Thank you