May 31 – June 2, Oslo Spektrum

10th anniversary

How to Create an Azure AD Protected API in an hour!

Jan Vidar Elven
Tech Lead Cloud Platform & Security
MVP Enterprise Mobility

Warning!

There will be code!

I will run out of time!

Let’s first talk about APIs..

Characteristics of APIs..

- What is an API?
  - Platform independence
  - Service evolution
- The RESTful API
  - HTTP
  - Resource
  - HTTP verbs
  - JSON data exchange
  - Stateless
  - Idempotent

https://docs.microsoft.com/en-us/azure/architecture/best-practices/api-design

RESTful API example..

- https://<your-web-api>/<version>/<resource>
  - CRUD (Create, Read, Update, Delete)
  - GET | POST | PUT | PATCH | DELETE

- Example Microsoft Graph API:
  - https://graph.microsoft.com/v1.0/users/<userid>

Azure AD Protected APIs..

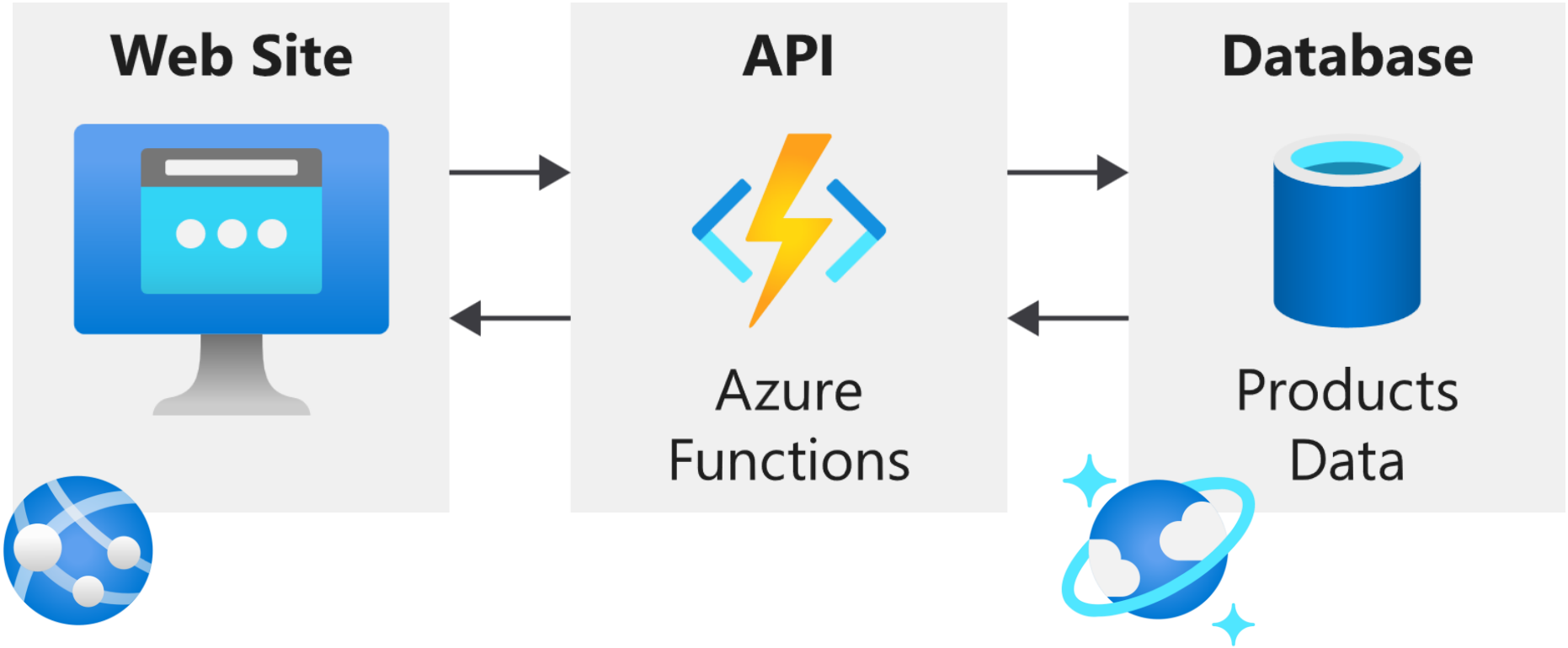
- Microsoft APIs
- Organization/Third-Party APIs
- Your Own APIs..

App Services

Azure Functions

Logic Apps

Demo Scenario – Azure Functions API



Demo Components

- Web Site:
  - Single-Page Application (SPA) built with Node.js, Vue & Axios (Microsoft Learn Identity Sample)
- API:
  - Azure Functions with PowerShell Core 7
- Database:
  - Cosmos DB Account with SQL API Container

Demo Tools and Environment

- Visual Studio Code.
  - https://code.visualstudio.com/
- Node.js.
  - https://nodejs.org/en/
- Azure Function Core Tools.
  - https://github.com/Azure/azure-functions-core-tools
- Azure Function Extension.
  - https://marketplace.visualstudio.com/items?itemName=ms-azuretools.vscode-azurefunctions
- PowerShell Core
  - https://github.com/PowerShell/PowerShell
- Postman
  - https://www.postman.com/downloads

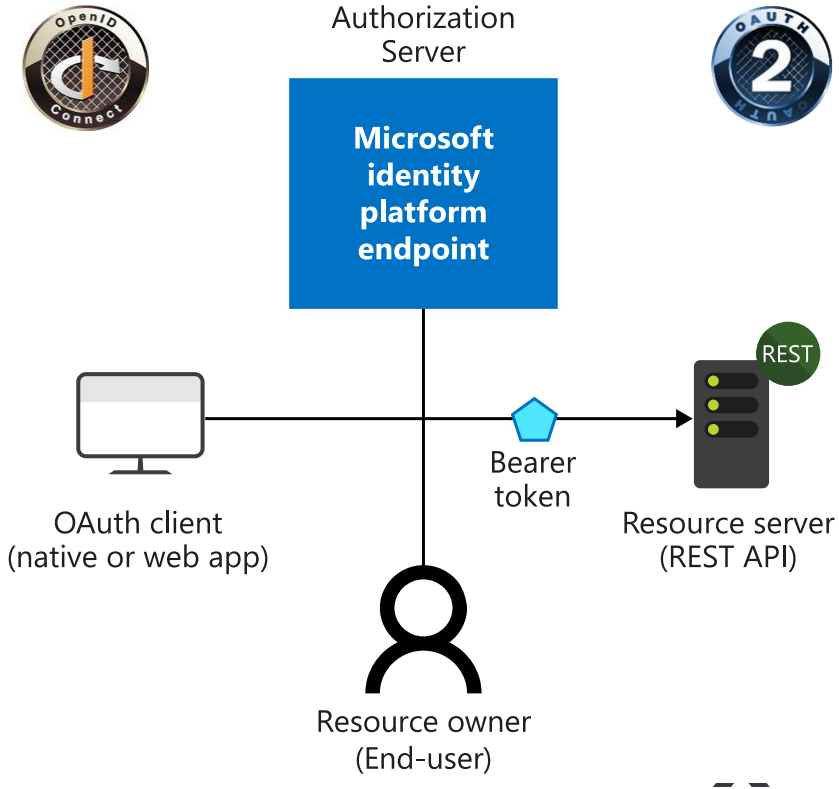
& access to an Azure Subscription and Azure AD Tenant..

Protecting API with Azure AD

OAuth2, OIDC and App Registrations

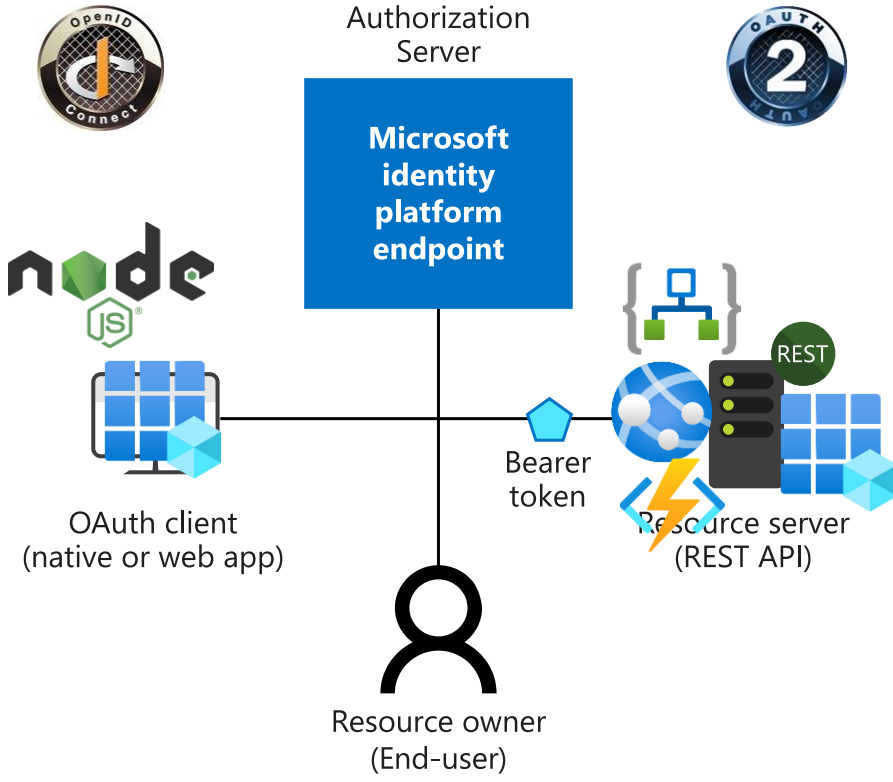
OAuth2 and OpenID Connect..

- AuthN & AuthZ
  - OpenID Connect (OIDC) for Authentication
  - Oauth 2.0 for Authorization
- Roles in OAuth 2.0 ->



APIs and OAuth2..

- App Registration in Azure AD represent the Client
- Application API Permissions represent resource API
- Functions App for AuthN & AuthZ
- Node.js web via Client
- End-user access via MSAL



How to setup for Function App API..

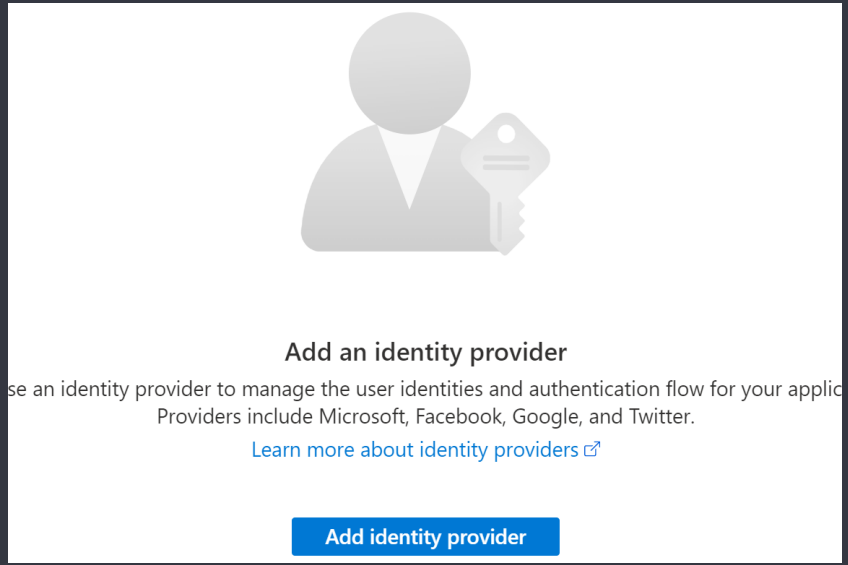
- Create App Registrations in Azure AD
  - API App Registration (expose API and represent Resource)
  - Client App Registration (represent Frontend)
- Add Function App API **Delegated** Permission(s)
  - api://<yourcustomapi>/<scopes>
- Admin or User Consent for Scopes?
- Optionally add Roles
- Add Authentication to Function App

Demo Scenario – Authorization

Implement AuthZ in Functions App for API requests

Azure Functions Authentication

- Require App Service Authentication/Authorization for Functions API requests
- Azure AD / Microsoft Identity
  - .. Other social providers available..
- https://docs.microsoft.com/en-us/azure/app-service/overview-authentication-authorization



Demo Scenario – Authentication

Implement AuthN in Functions App for API requests

Demo Scenario – Web Frontend

Implement MSAL in Node.js Web frontend for API Requests

Resources

- https://docs.microsoft.com/en-us/learn/modules/build-api-azure-functions/
  - https://github.com/MicrosoftDocs/mslearn-build-api-azure-functions
- https://docs.microsoft.com/en-us/azure/architecture/best-practices/api-design
- https://github.com/JanVidarElven/build-azure-ad-protected-api-azure-functions
- https://gotoguy.blog/2021/12/22/creating-an-azure-ad-protected-api-in-azure-in-a-school-hour/

Connect

Jan Vidar Elven

@JanVidarElven

gotoguy.blog

Slides and demos from the conference will be available at

https://github.com/nordicinfrastructureconference/2022