Securing the API (OAuth 2.0 and OpenID Connect)

Kevin Dockx

@KevinDockx | http://blog.kevindockx.com/

Calling the API on Behalf of the User

Learn how to use resource scopes to secure the API

Role-Based Authorization

Learn how to use role-based authorization at API level

User-Specific Data – API Responsibility

Learn how to request data belonging to the authenticated user, putting the responsibility on the API

Client Credentials: Server to Server

Learn how to use the Client Credentials flow to secure the API

API Access Through Implicit Flow

Learn how to securely access the API
from our Windows Phone client

Refresh Tokens

Learn how to request a refresh token
for long-lived access

Summary

We can secure the API through a resource scope

We can authorize access

- by passing the users' roles & using claims
- with additional scopes (machine-to-machine)

We can leverage claims for user-specific data

To refresh an access token, refresh tokens can be used

When in doubt, use standards

When not in doubt, use standards as well

The thing with security is that a lot of approaches will work, but most are not a good idea

You’re ready to be AWESOME!