Securing ASP.NET Core 6 with OAuth2 and OpenID Connect

Getting Started with ASP.NET Core Security

Kevin Dockx
Architect

@KevinDockx https://www.kevindockx.com

Securing ASP.NET Core 6 with OAuth2 and OpenID Connect

Version Check

Version Check

This version was created by using:

- ASP.NET Core 6.0.6
- Duende.IdentityServer 6.1.1
- .NET 6.0
- Visual Studio 2022

Version Check

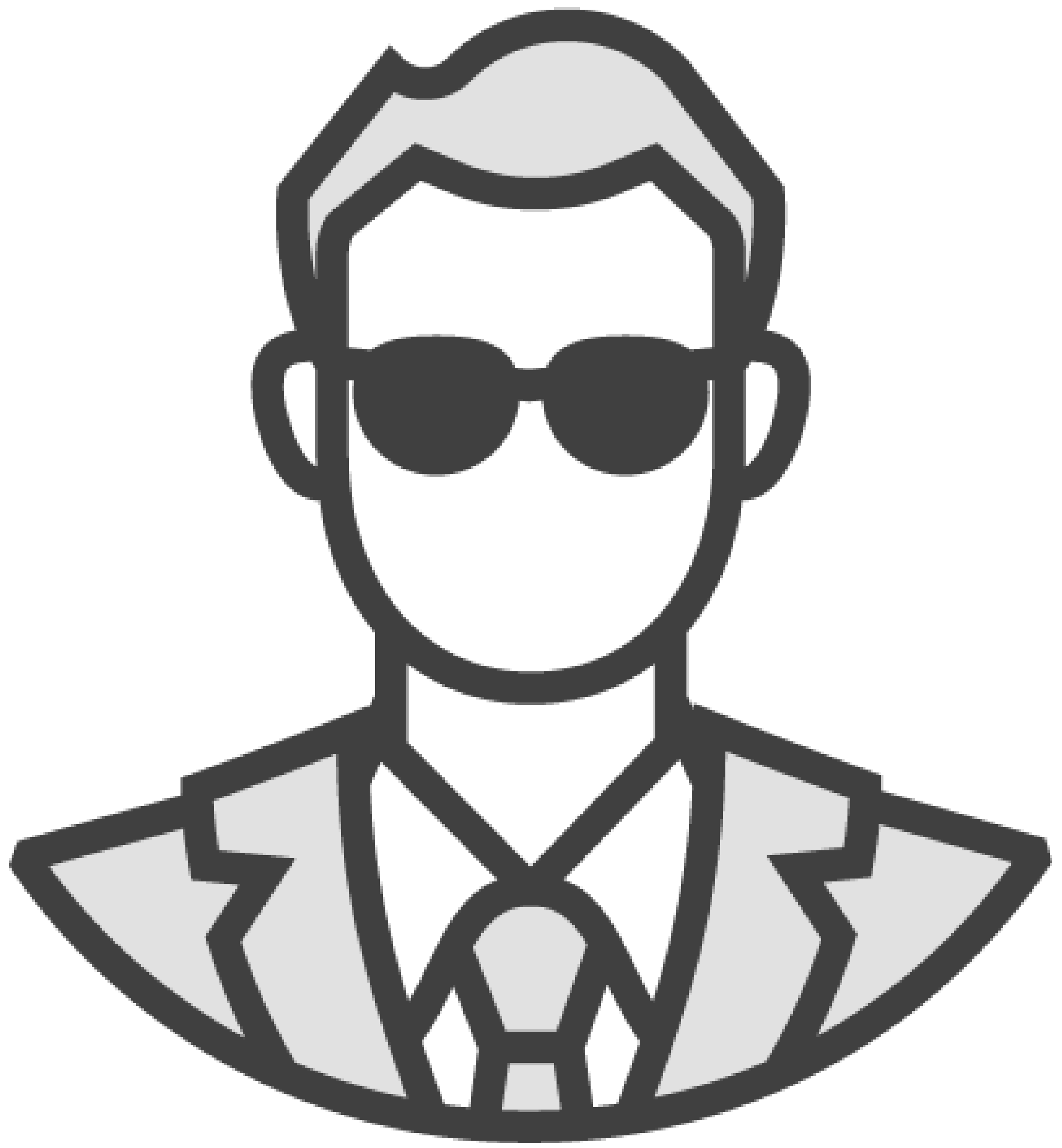
This course is 100% applicable to:

- ASP.NET Core 6.x, 7.x
- Duende.IdentityServer 6.x
- .NET 6.x, 7.x

Relevant Notes

New course versions are regularly released:

- https://app.pluralsight.com/profile/author/kevin-dockx



Knowing how to secure applications is important…

… but knowing why you (should) make certain decisions is, arguably, even more important

Coming Up

Positioning this course

Course prerequisites and tooling

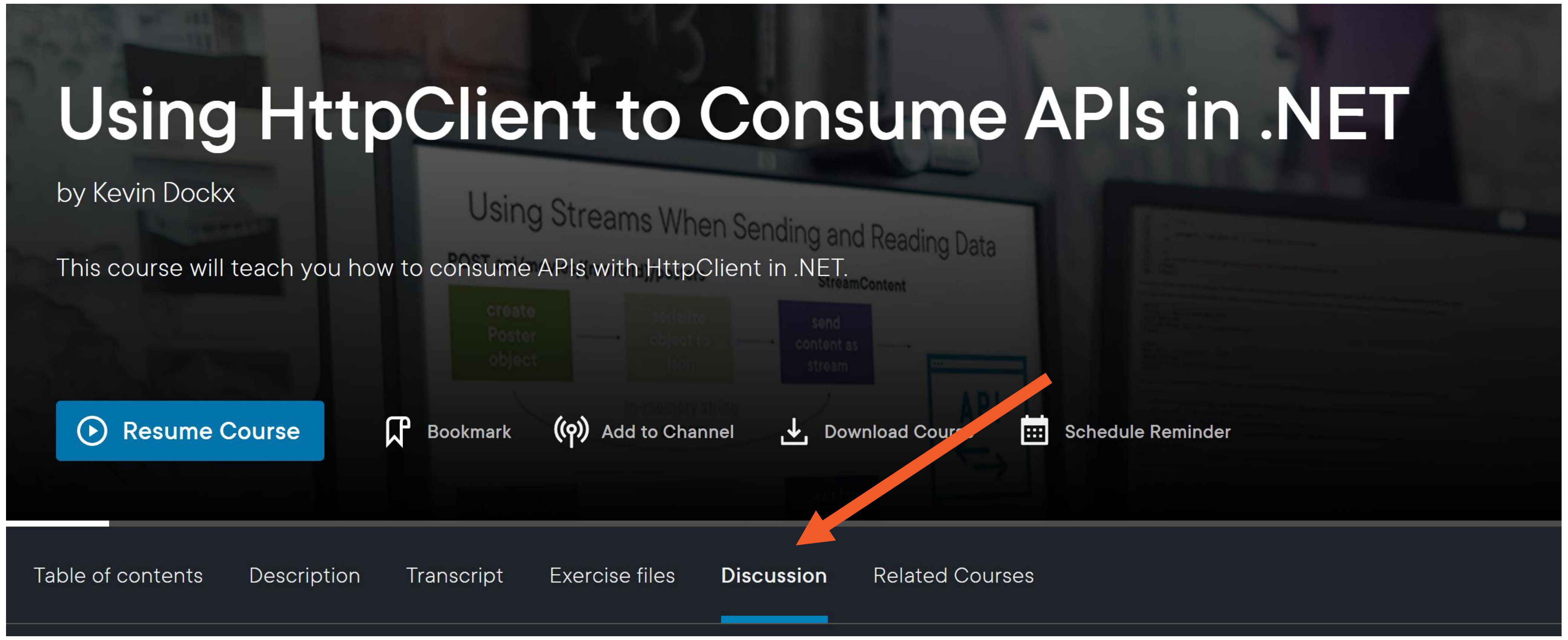
Application architectures and security

The importance of a central identity provider

Introducing OAuth2 and OpenID Connect

Discussion tab on the course page

Twitter: @KevinDockx


Using HttpClient to Consume APIs in .NET

by Kevin Dockx

This course will teach you how to consume APIs with HttpClient in .NET.

(course shown is one of my other courses, not this one)

Positioning This Course

Integrating user authentication in your client applications

Securely accessing APIs from those client applications

Integrating an identity provider with a user database and other identity providers

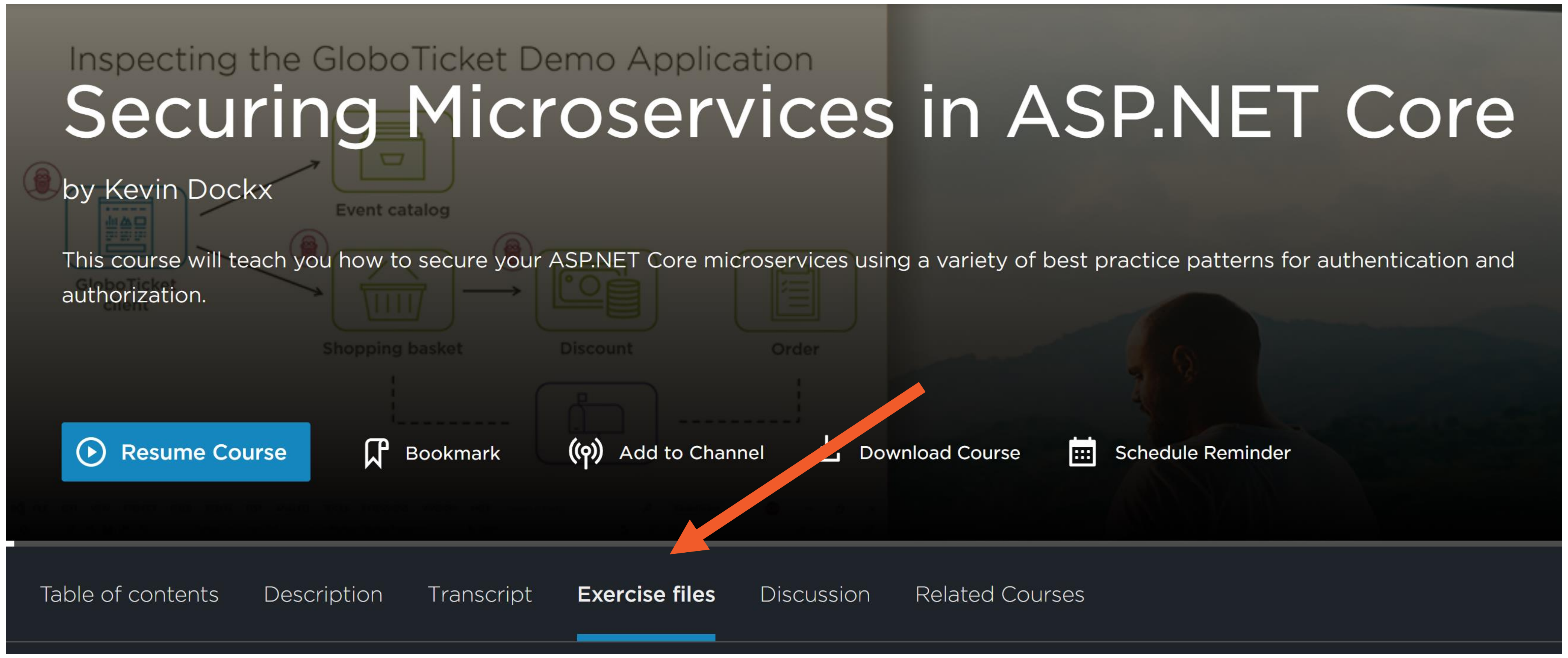
Getting ready for production and deploying your identity provider

Course Prerequisites

Good knowledge of C#

Some knowledge of building ASP.NET Core 6 web applications and/or web APIs

Exercise files tab on the course page


Inspecting the GloboTicket Demo Application
Securing Microservices in ASP.NET Core
by Kevin Dockx
This course will teach you how to secure your ASP.NET Core microservices using a variety of best practice patterns for authentication and authorization.
Resume Course
Bookmark
Add to Channel
Download Course
Schedule Reminder
Table of contents
Description
Transcript
Exercise files
Discussion
Related Courses

(course shown is one of my other courses, not this one)

Application Architectures and Security

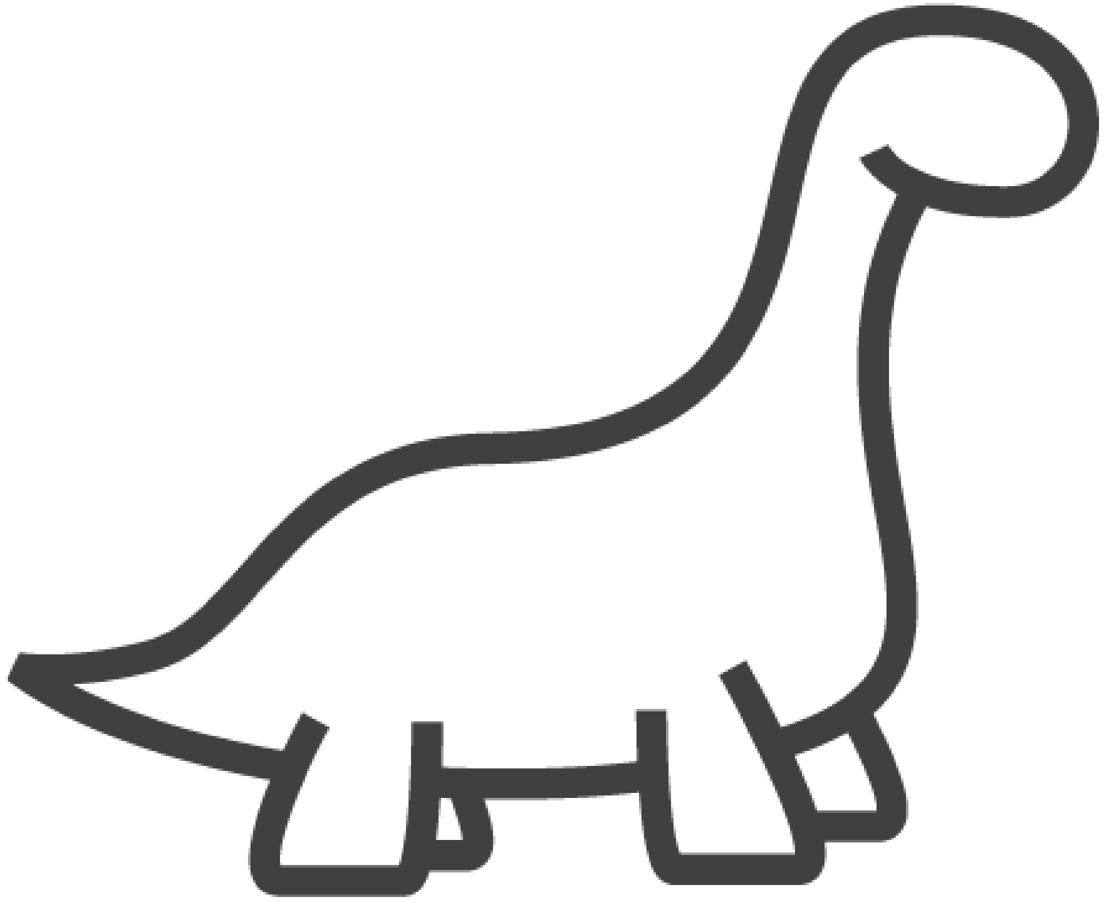
Thick client applications

- Windows authentication

Server-side web applications

- Windows or Forms authentication

Not service-based



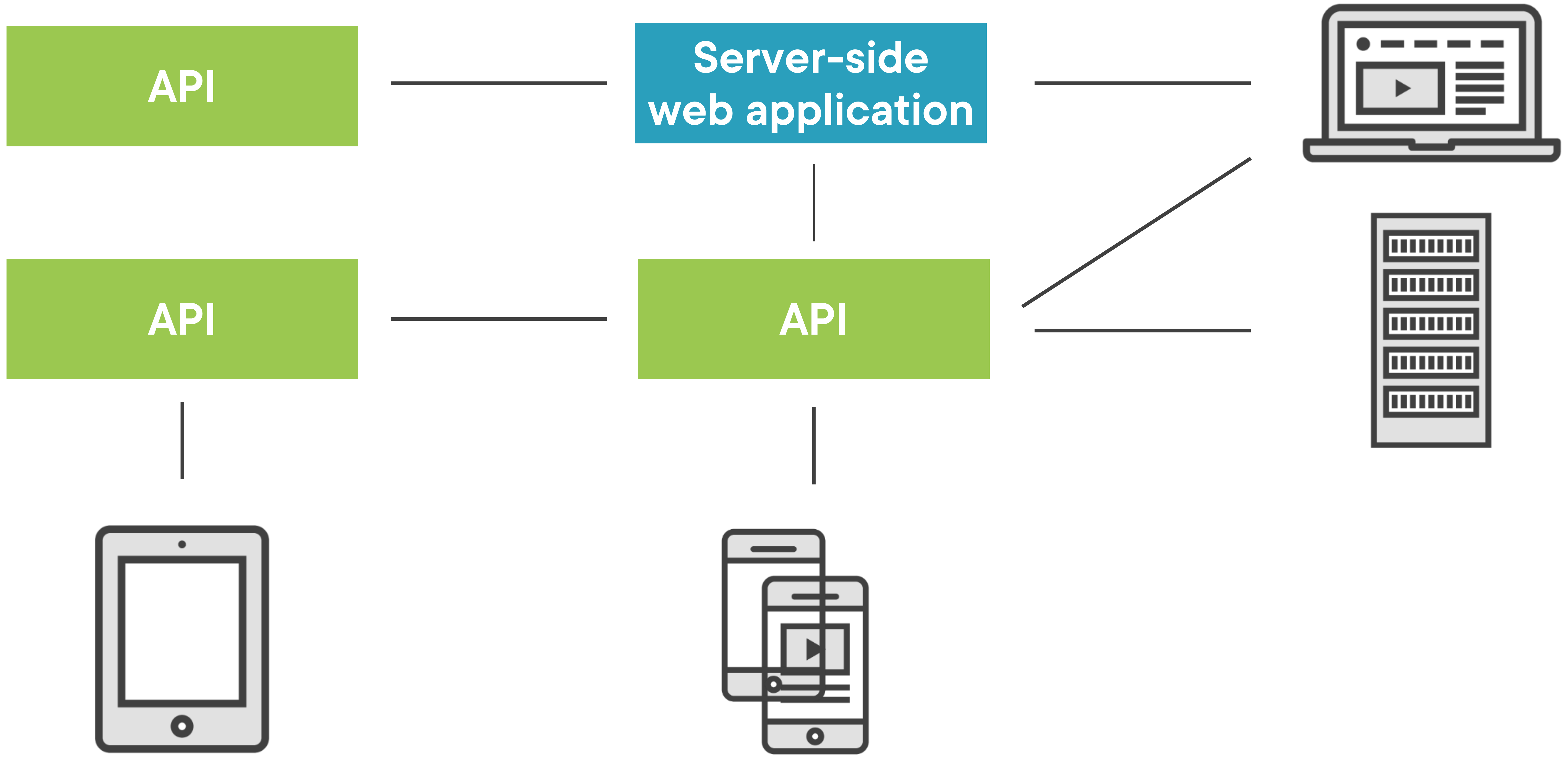
Service-based applications

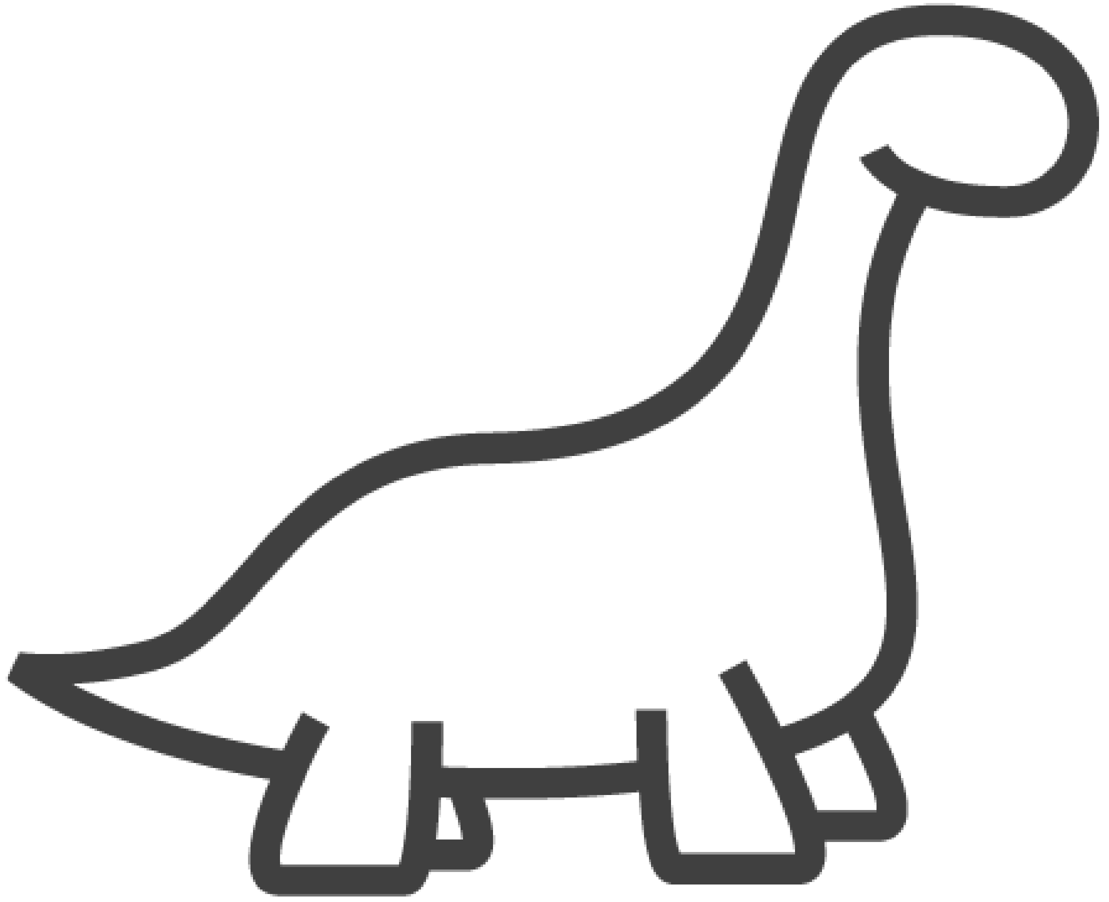
- WS-Security (WCF)
- IP-level configuration (firewall)

SAML 2.0

- Standard for exchanging authentication and authorization data between security domains

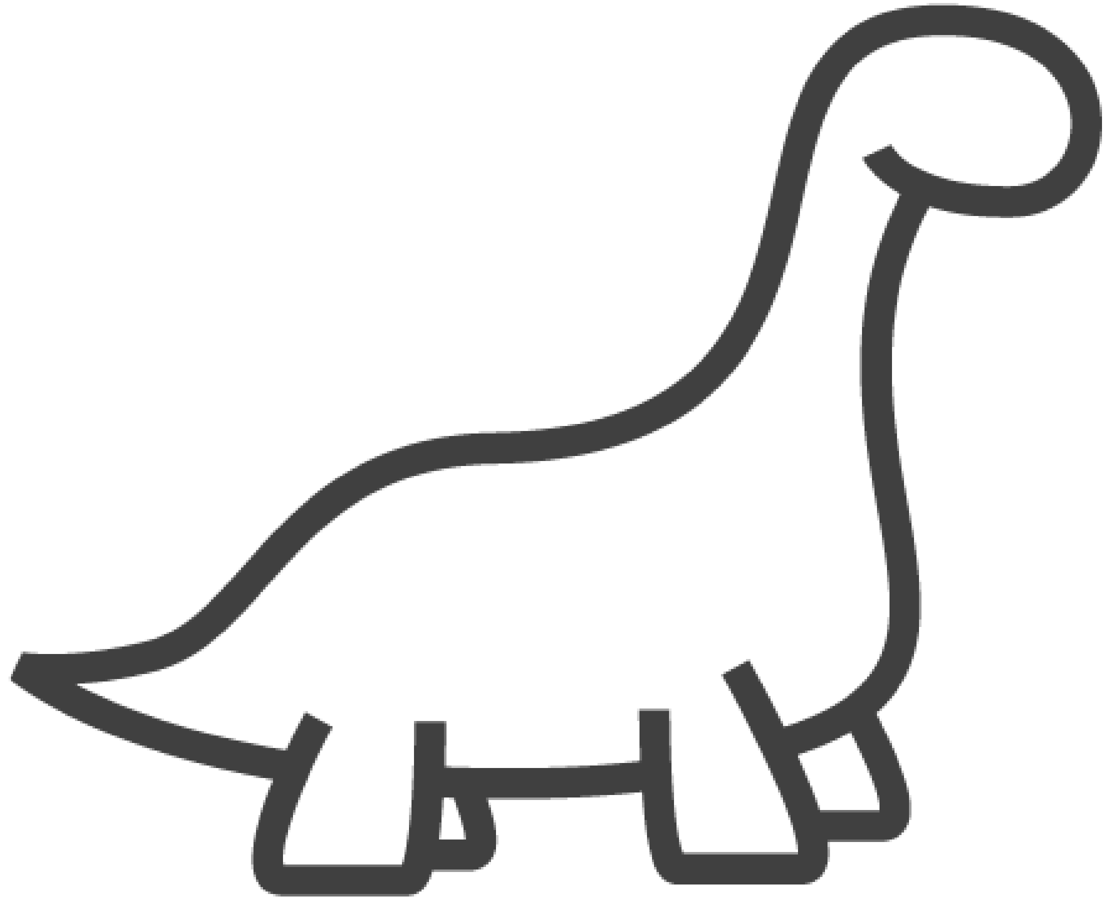
Application Architectures and Security



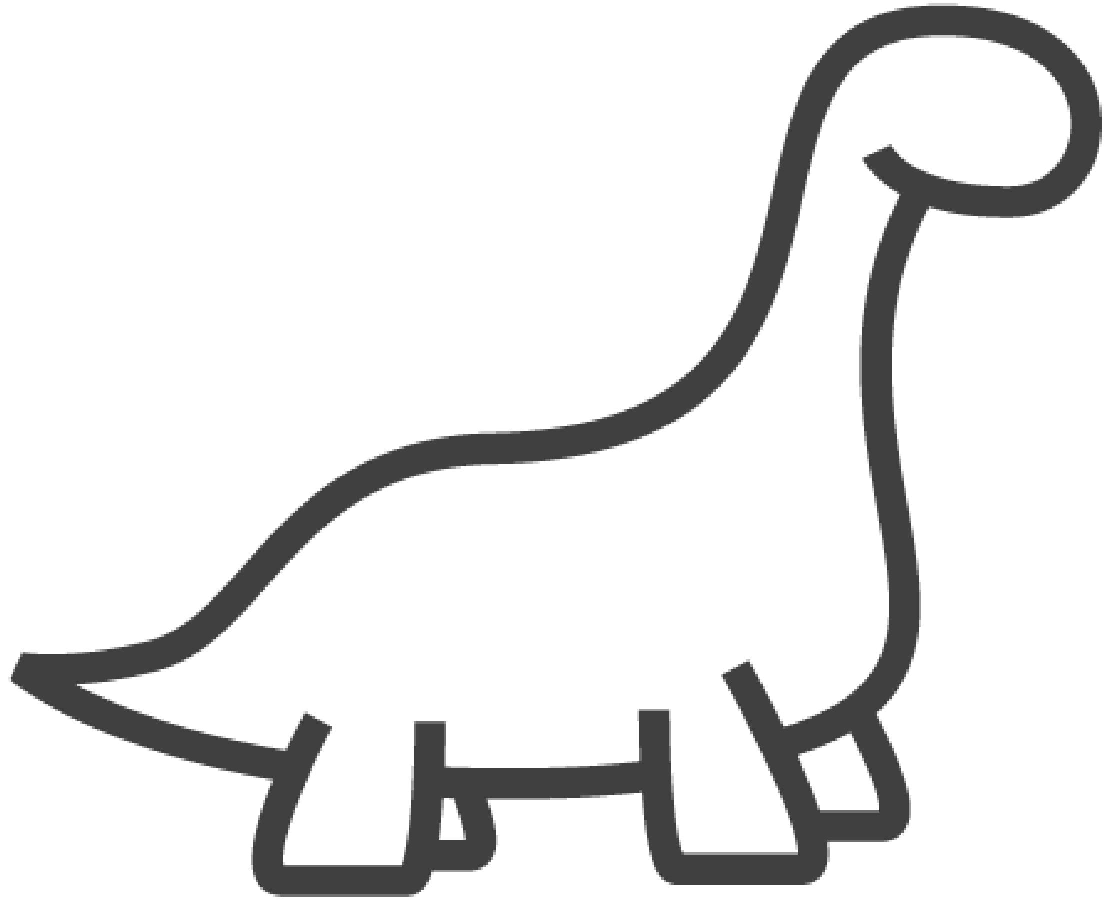


Client applications (often) require public APIs

Applications that live on the client can’t be (decently) secured with means designed for use at the server



Sending username/password on each request proved to be a bad idea



Token-based security

- Client applications send tokens, representing consent, to API

Home-grown token services emerged…

- The application still has access to username/password

Expiration

Token signing and validation

Token format

Authentication and authorization

Securely delivering tokens to different application types

...

Application Architectures and Security

A central identity provider

A protocol that's safe for authentication and authorization

Working Towards a Central Identity Provider

It’s the responsibility of an Identity Provider (IDP) to authenticate the user and, if needed, safely provide proof of identity to an application

IAM (Identity and Access Management)-related Tasks

- User registration & management
- Locking out users
- Password policies, strength & resets

… are tedious tasks, prone to change

Handle them in a central location and reuse them across applications

Early-days encryption mechanism can easily be brute forced

- Key stretching algorithms discourage this…
- … but the amount of stretching and the algorithms themselves are prone to change

Some systems might require certificates

Other systems might require a second or third factor of authentication

User accounts are reused across applications

Identity and access management-related tasks are common concerns

Safely storing account-related information is prone to change

Means of authentication are added or changed

Working Towards a Central Identity Provider

A central Identity Provider (IDP), as part of an Identity and Access Management (IAM) system, solves these issues

Expiration

Token signing and validation

Token format

Authentication and authorization

Securely delivering tokens to different application types

...

OAuth2

OAuth2 is an open protocol to allow secure authorization in a simple and standard method from web, mobile and desktop applications

Introducing OAuth2

A client application can request an access token to gain access to an API

- OAuth2 defines how a client application can securely achieve authorization

Introducing OAuth2

Homegrown endpoints are replaced by endpoints from the OAuth2 standard

The standard defines how to use these endpoints for different types of client applications

Introducing OAuth2

Identity providers like Duende.IdentityServer, Azure Active Directory, … implement the OAuth2 standard

- Others include Ping, Okta/Auth0, WSO2 IdentityServer, TrustBuilder, …

OpenID Connect

OpenID Connect is a simple identity layer on top of the OAuth2 protocol

Introducing OpenID Connect

A client application can request an identity token (next to an access token)

That identity token is used to sign in to the client application

Introducing OpenID Connect

OpenID Connect is the superior protocol: it extends and supersedes OAuth2

- Once you deal with users, use OpenID Connect

Introducing OpenID Connect

OIDC isn’t just for new or API-based applications

Demo

Introducing the demo application

Summary

Identity and Access Management (IAM) belongs at a central location

- A central Identity Provider (IDP) is part of such an IAM system

That IDP must implement protocols that safely allow authentication and authorization: OpenID Connect & OAuth2

Up Next:
Understanding Authentication with OpenID Connect