Authorizing Calls to Your Backend APIs with OAuth 2

Brian Noyes
CTO, SOLLIANCE INC

@briannoyes www.briannoyes.com

Module Overview

OAuth 2 Protocol Overview

Authorizing Calls with OAuth 2 Access Tokens in the Client

Adding Filtering and Access Control in ASP.NET Core

OAuth 2 Terminology / Roles

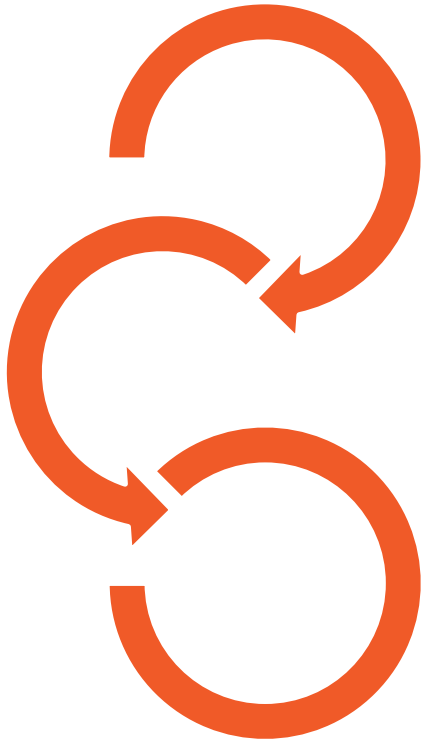
Resource Owner

Resource Server

Client

Authorization Server

OAuth 2 Grant Types



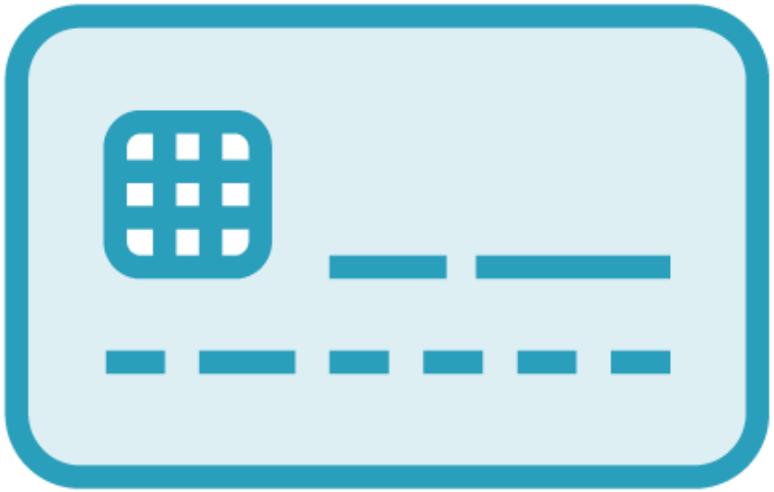
- Implicit
- Authorization Code
- Resource Owner Password Credential
- Client Credential

OAuth 2 Token Types

Access Token

Refresh Token

Access Token Contents



- Client ID (client_id)
- Subject ID (nameidentifier)
- Issuer (iss)
- Issue timestamp (nbf)
- Expiration timestamp (exp)
- Scope claims (scope)
- Additional claims

Resource Server Responsibilities

Decode Token

Validate Token

Authorize Calls

Expose Security Context API for Client

Refresh Tokens

Not applicable to Implicit flow clients

Requires secure storage of refresh token

Silent renewal of access token with Implicit clients

Demos

Starting point: Authentication complete

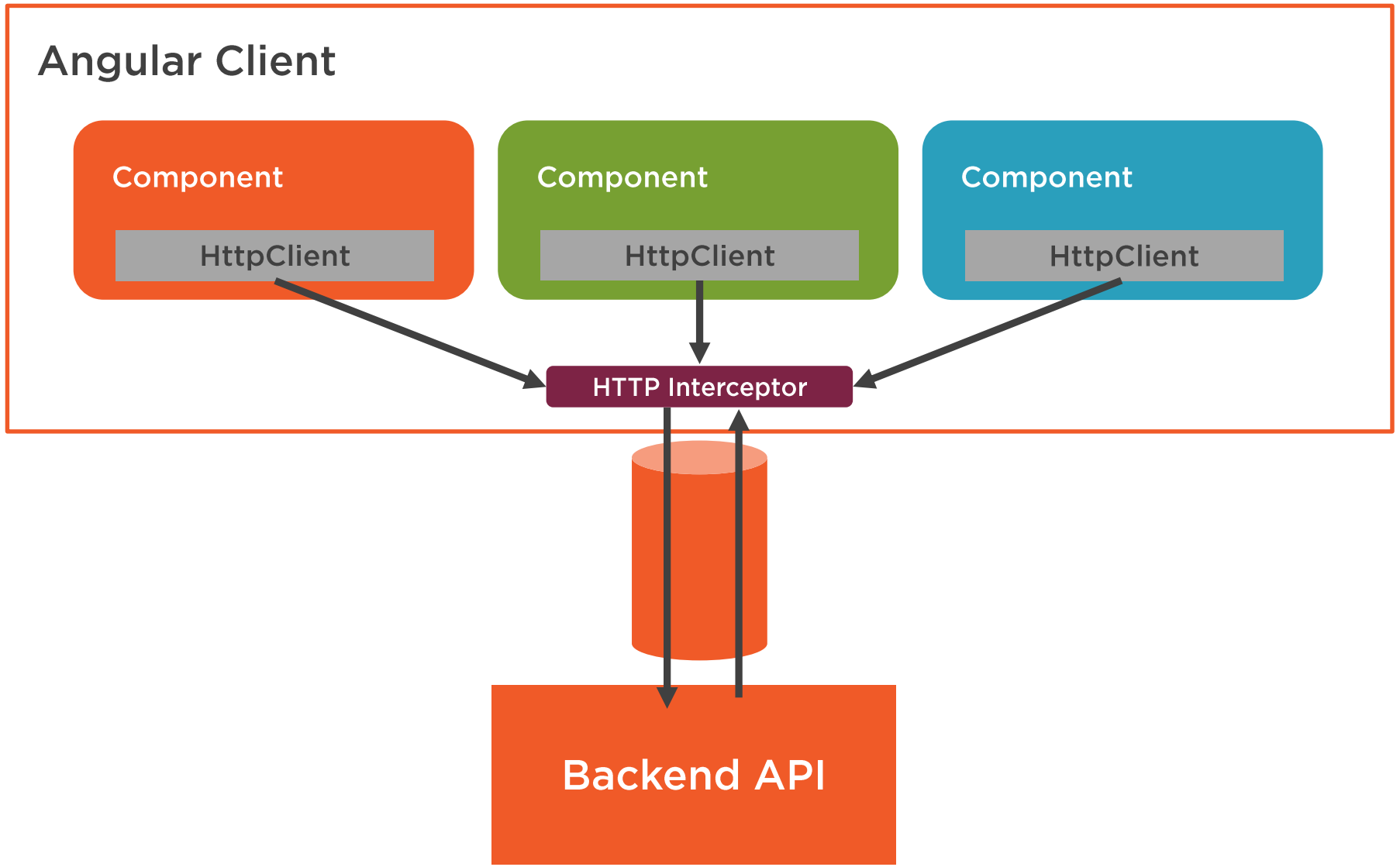
Pass access tokens to API

Require authentication/authorization in APIs

Filter data on back end

Control access to operations

HTTP Interception



Summary

Pass OAuth 2 access tokens to API

HTTP interceptor

- Add tokens to Authorization header
- Handle authorization error responses

API enforcement of access control

Add custom identity claims