Setting Up a BFF with OAuth2 and OpenID Connect

Roland Guijt

Freelance consultant and trainer

@rolandguijt | roland.guijt@gmail.com

Backend Technology

ASP.NET Core

Many other platforms

Concepts should be similar

https://4sh.nl/angularcode

Steps Before Running

Install .NET SDK

- https://4sh.nl/dotnet

Install/update node.js

- https://nodejs.org

Install npm packages

How to Create a BFF

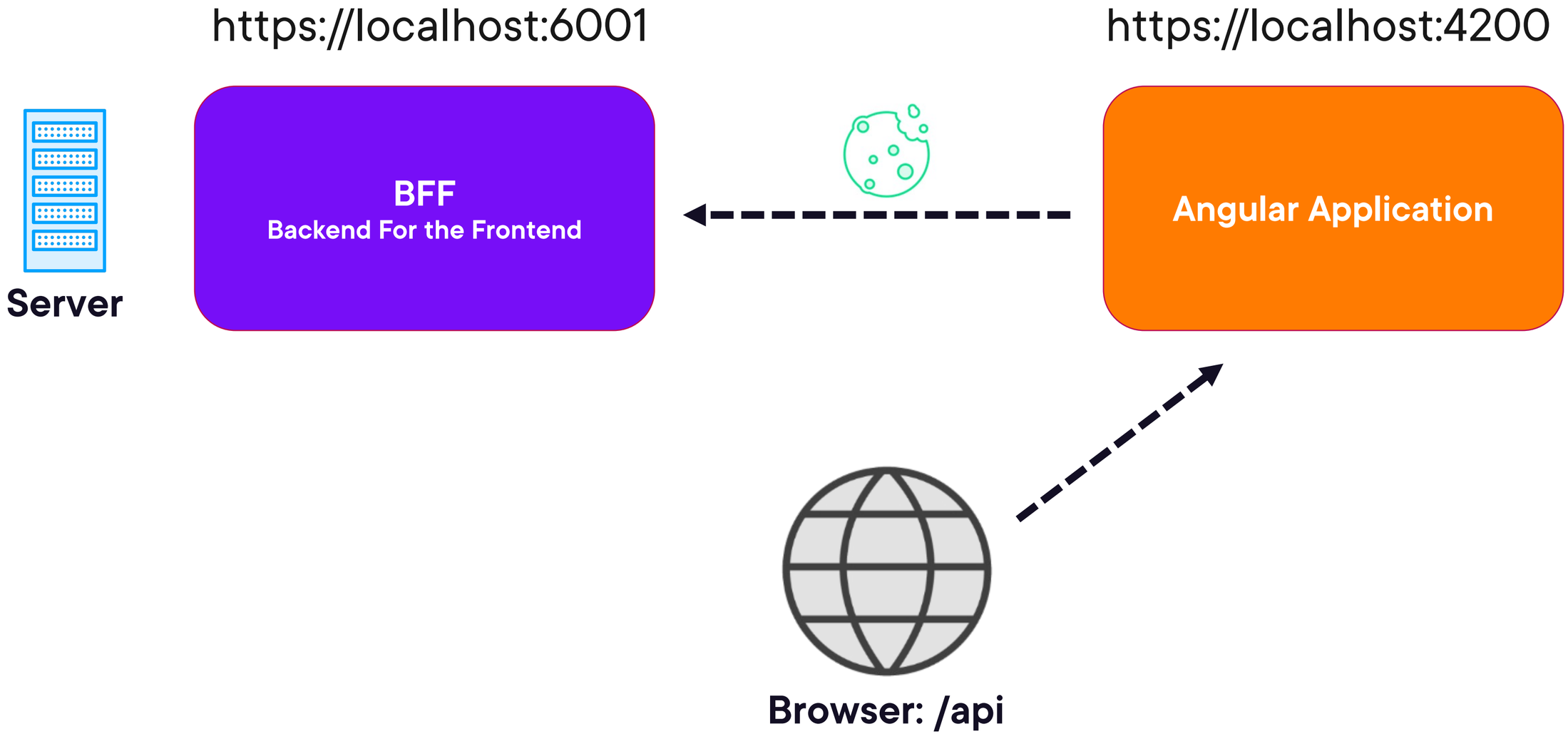
Using Duende BFF (for ASP.NET Core) in the example code

Other libraries on other platforms available

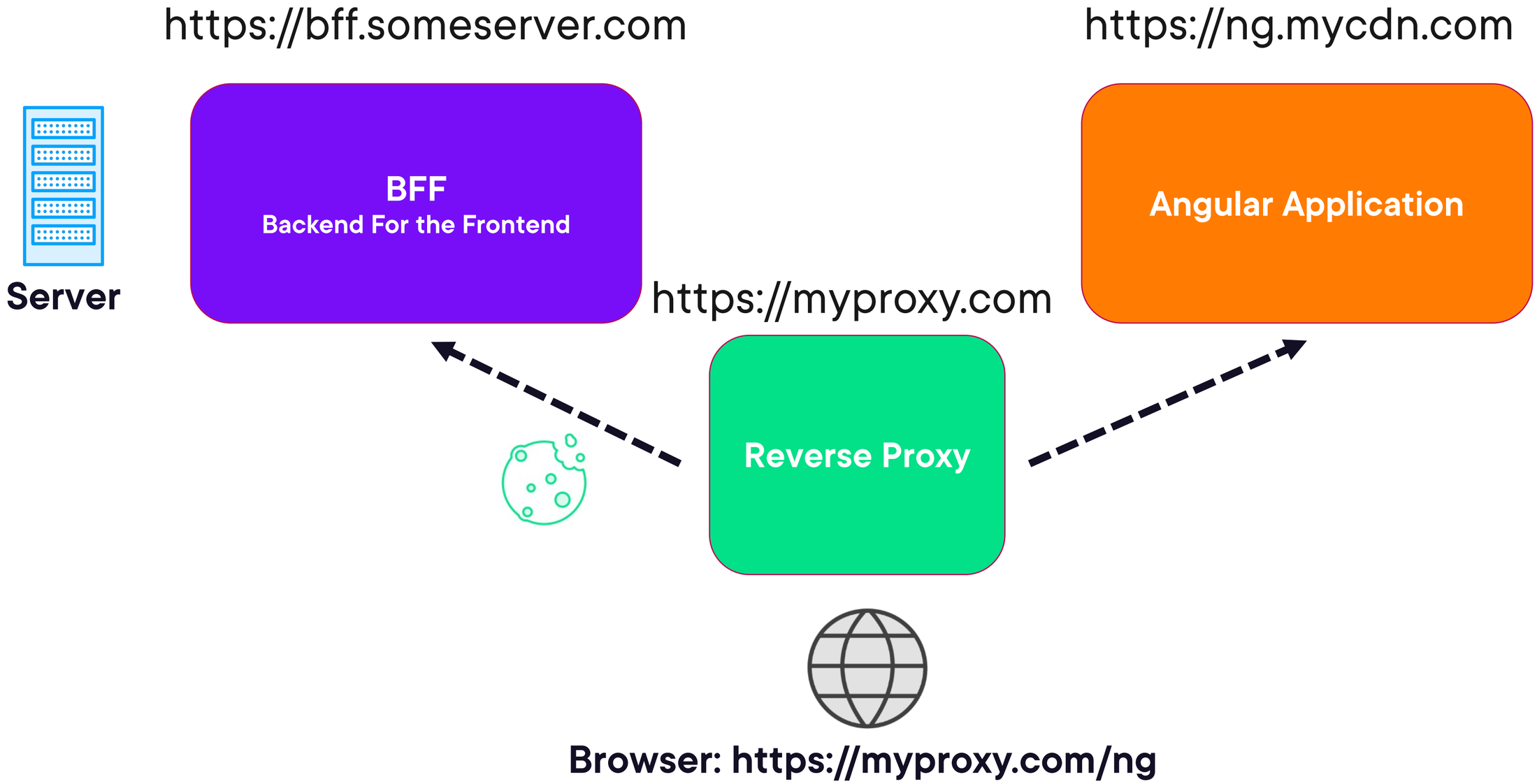
Writing your own is an option

https://4sh.nl/strictcookie

Angular's Reverse Proxy



SameSite Cookies with Reverse Proxy



Sending a Custom HTTP Header

Any custom header will trigger a CORS preflight request

Attackers are required to send the header, rejecting the request before it is made

Extra CSRF protection on top of SameSite cookies

Moving to OpenID Connect

No need from a security standpoint

But centralized authentication preferable

Ability to access external APIs

Authentication and Authorization in Angular

Token Management

Access token has limited lifetime

Refresh token can be requested with the offline_access scope

BFF library will automatically refresh if needed

Alternative: call token endpoint manually

Up Next:

Authorization with Route Guards and Conditional Rendering