Authorization Policies and Access Control

Kevin Dockx

Architect

@KevinDockx https://www.kevindockx.com

Coming Up

Attribute-based access control

Authorization policies

Role-based Access Control vs. Attribute-based Access Control

Role-based Access Control (RBAC)

Access rights granted through predefined roles

Each role carries a set of privileges

Attribute-based Access Control (ABAC)

Access rights granted through policies

A policy combines a set of attributes (claims) together

Allows much more complex rules than RBAC

Upcoming Demos

We'll replace RBAC with ABAC

Only users:

- that live in Belgium ("be")
- that are in role "PayingUser"

… will be allowed to add an image

Demo

Creating an authorization policy

Demo

Using an authorization policy (web client)

Demo

Using an authorization policy (API)

```
{
    ...,
    "aud": ["imagegalleryapi"],
    "scopes": ["imagegalleryapi.read", "imagegalleryapi.write"]
    ...
}
```

Fine-grained Policies with Scopes

Requesting imagegalleryapi.read and imagegalleryapi.write scopes

Scope-based authorization

This is about what a client application is allowed to do, not about who the end-user is

```
{
    ...,
    "aud": ["imagegalleryapi"],
    "scopes": ["imagegalleryapi.fullaccess"]
    ...
}
```

Fine-grained Policies with Scopes

Requesting just one scope: imagegalleryapi.fullaccess

```
{
     ...,

     "aud": ["imagegalleryapi"],

     "scopes": ["imagegalleryapi.read", "imagegalleryapi.write"]

     ...
}
```

Fine-grained Policies with Scopes

Requesting imagegalleryapi.read and imagegalleryapi.write scopes

Demo

Fine-grained policies with scopes

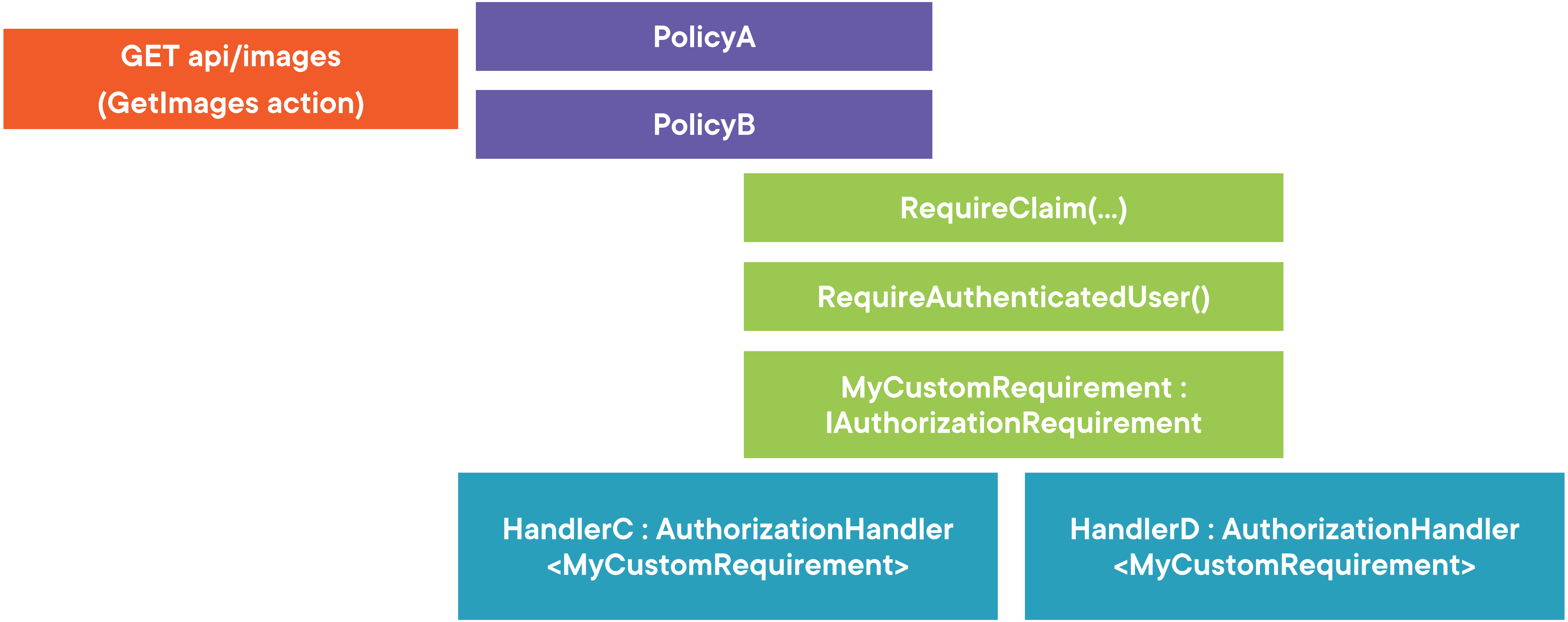
Extending Authorization Policies with Requirements and Handlers

Built-in policy options are great for simple cases

The need for more complex rules requires extending the policy

- Boolean operators
- Repository access
- Route data access
- …

Extending Authorization Policies with Requirements and Handlers



GET api/images

(GetImages action)

PolicyA

PolicyB

RequireClaim(...)

RequireAuthenticatedUser()

MyCustomRequirement : IAuthorizationRequirement

HandlerC : AuthorizationHandler <MyCustomRequirement>

HandlerD : AuthorizationHandler <MyCustomRequirement>

Demo

Creating custom requirements and handlers

Summary

Attribute-based access control (ABAC)

- Access rights granted through policies
- A policy combines a set of attributes (claims) together
- Allows much more complex rules than RBAC

ABAC is the preferred approach for most applications these days

Up Next:

Dealing with Token Expiration, Reference Tokens and Token Revocation