Applying Authorization

Roland Guijt
MICROSOFT MVP, CONSULTANT, AUTHOR AND SPEAKER

@rolandguijt rolandguijt.com

Overview

Different ways to do authorization:

- Claims based
- Role based
- Resource based
- View based

In different application types:

- Web
- APIs

[Authorize] Hierarchy

```
[Authorize]
public class ConferenceController: Controller

        [Authorize(Policy = "CanAddConference")]
        public Task<IActionResult> Add()
```

What if a policy with more complexity is needed?

A More Complex Policy

Speakers may only add a new proposal when they have more than the specified years of experience

Calculate years of experience using CareerStarted claim

Compare calculated years with specified number of years

Requirements and Handlers

YearsOfExperienceRequirement

YearsOfExperience = 5

AuthorizationHandler<YearsOfExperienceRequirement>	Succeed Fail Do nothing
AuthorizationHandler<YearsOfExperienceRequirement>	Succeed Fail Do nothing

Logic Around Multiple Handlers and/or Policies

If no handler calls Succeed, access is denied

If one of them calls Fail, access is denied

Calling Fail explicitly denies access, no matter what other handlers and policies do

But they are still called

Multiple Handlers

Badge

Visitor sticker

New Resource-based Policy

Purpose: May a proposal be edited?

Depends on Approved property on proposal

Instance of proposal is needed

Benefits of Resource-based Policies

Centralized

Reuse

Enables complex logic

Can be used on any kind of object

Authorization Data

Identity Token is about the user's identity

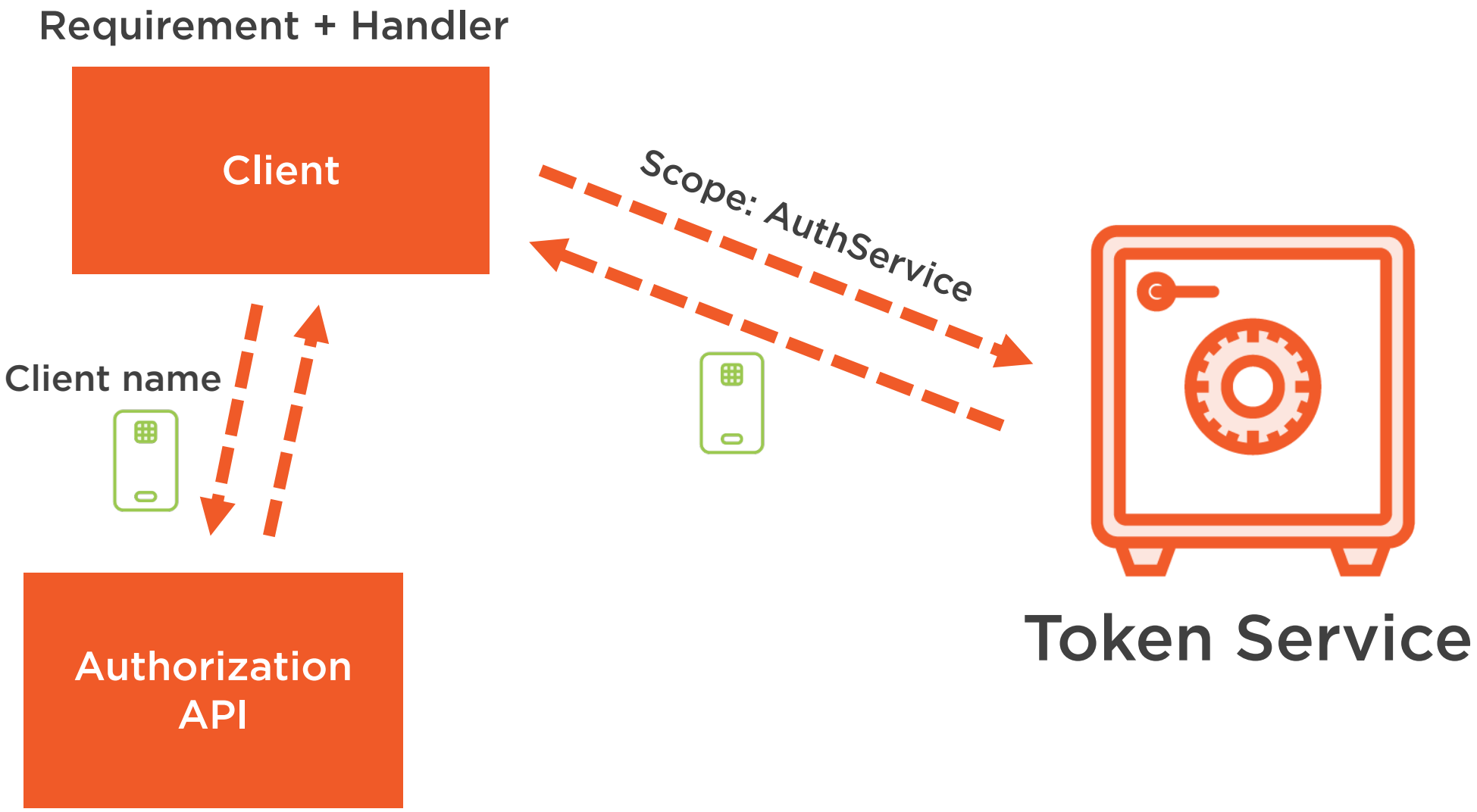
Not Authorization Data

Bloated identity token could cause problems

Context for each client or API is different

Suggestion: Create Authorization API

Architecture With Authorization API



Summary

Creating and applying centralized policies is the way to go

Use them in web applications and APIs

Protecting resources

Where do you get the authorization data?

Roland Guijt

Microsoft MVP, consultant, author and speaker

@rolandguijt rolandguijt.com

roland.guijt@gmail.com