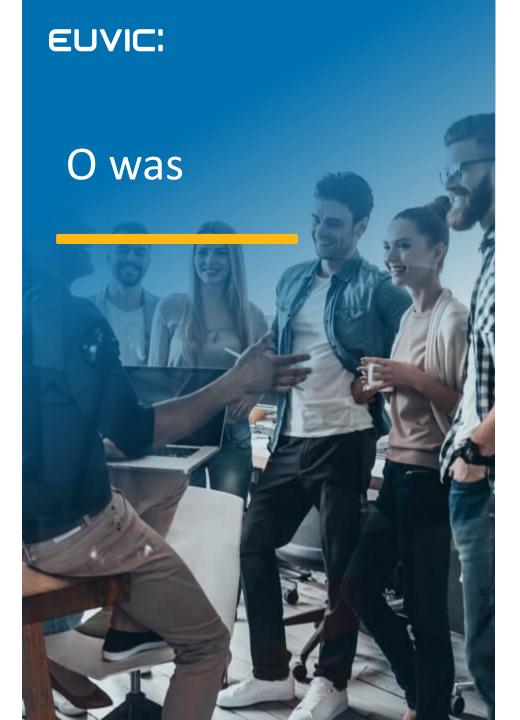
# EUVIC: THE GOOD People

WebAPI
Uwierzytelnianie i
Autoryzacja



Kilka słow o mnie



# Odpowiedź na pytania:

- Jak długo zawodowo pracujesz jako programista
- Jaka jest Twoja główna technologia
- Z kąd się do nas łączysz



## Zapiszcie na czacie

z jakiej technologi tożsamości (identity provider)

korzystasz w swoim obecnym lub poprzednim projekcie



Czym jest Uwierzytelnianie

Czym jest Autoryzacja



Czym jest Uwierzytelnianie Czym jest Autoryzacja

Jakie są wasze odpowiedzi



# Czym jest uwierzytelnianie Proces w którym potwierdzamy kim jest użytkownik

Czym jest autoryzacja

Proces kontroli dostępu użytkownika do zasobu



# Uwierzytelnianie czy Autoryzacja

- Użytkownik loguje się za pomocą loginu i hasła do systemu
- Użytkownik wchodzi do pokoju używając skanera lini papilarnych
- Potwierdzenie przelewu w banku za pomocą palca
- Uzycie karty kredytowej do zaplacenia za zakupy
- Wpisanie kodu (np. z google auth) do VPN
- Użytkownik loguje się do windowsa za pomocą skanu swojego palca
- Wpisanie kodu który przyszedł na maila gdy mamy 2-FA
- Ochroniarz wpuszcza pracownika po zobaczeniu jego karty



## A jak to jest w kodzie?

https://github.com/aspnet/Security/blob/1c30f33 c925a97b105b3f9d34497218b0c9342b6/src/Micr osoft.AspNetCore.Authentication/Authentication Middleware.cs

Authentication Middleware ✓

Authorization Middleware ✓



#### Podsumowanie

Uwierzytelnianie - proces w którym potwierdzamy kim jest użytkownik

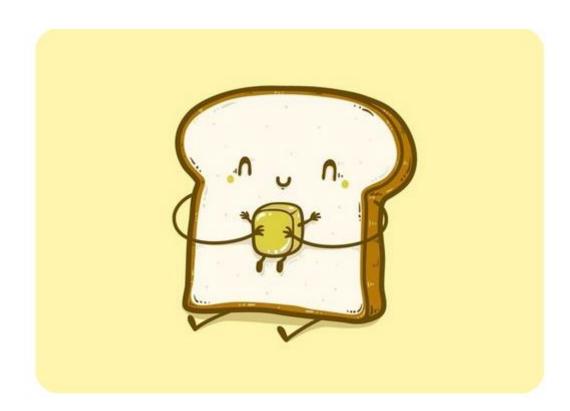
Autoryzacja - proces kontroli dostępu użytkownika do zasobu

app.UseAuthentication() – middleware do uwierzytelniania

app.UseAuthorization() — middleware do autoryzacji



# To wszystko bułka z masłem



#### **EUVIC:**

#### Metody uwierzytelniania

Kto w obecnym projekcie korzysta z JWT Token

A kto w obecnym projekcie dostaje cookie jako rezultat uwierzytelnienia

Wnioski?



#### Metody uwierzytelniania

#### Cookie

- Może mieć termin ważności
- Jest powiązane z sesją (Stateful)
- Jest akceptowane tylko przez subdomeny
- Jest trzymany w przeglądarce
- Maksymalny rozmiar 4kb
- Można unieważnić cookie po stronie serwera
- Z powodu sesji źle się skaluje



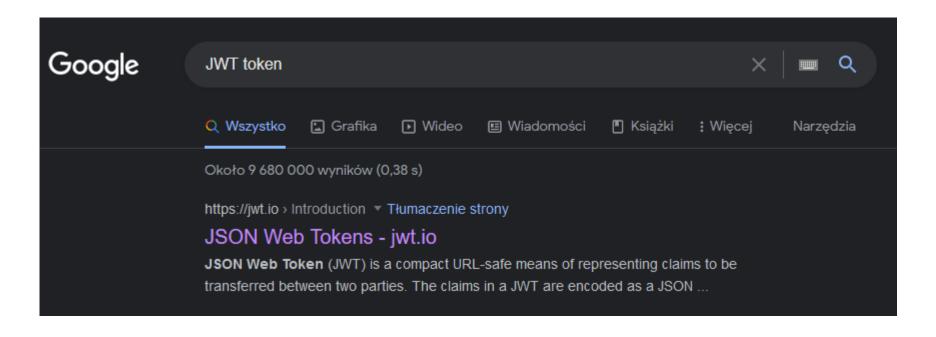
#### JWT Token

- Ma termin ważności
- Brak mechanizmu sesji (Stateless)
- Ten sam token może być akceptowany w różnych domenach
- Może być zapisany w kodzie lub local/session storage
- Maksymalny rozmiar jest ograniczony przez rozsądek
- Serwer nie ma możliwości unieważnienia tokena
- Nie ma negatywnego wpływu na skalowanie systemu



### Metody uwierzytelniania

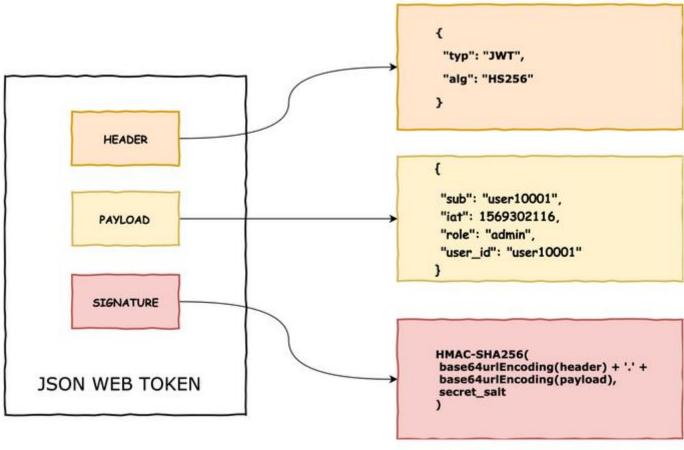
#### Kto zna te narzędzie?





### Struktura tokena







Jak zdobyć token aby użyć go potem w postmanie?



Jak skorzystać z postmana aby zrobić request do API





#### Metody uwierzytelniania

#### Wnioski

Czy ktoś zauważył jak przesylany jest token?

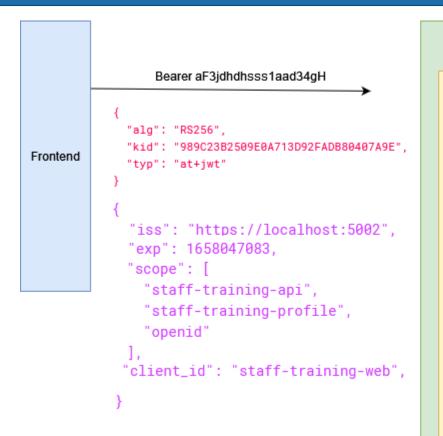
#### Curl

curl -X GET "https://kp-staff-training.azurewebsites.net/api/attendees" -H "accept: text/plain" -H "Authorization: Bearer
eyJhbGciOiJSUzI1NiIsImtpZCI6IjUwMzFDN0MxNDMxRThDQTcwMDI0RTBDM0VDMjQyODA0IiwidHlwIjoiYXQrand0In0.eyJpc3MiOiJodHRwczovL2twLWlkZW50aXR5c2VydmVyLmF6dXJld2Vic2l0ZXMubmV0IiwibmJmIjoxNjU4MTI1MTk3LCJpYXQ
iOjE2NTgxMjUxOTcsImV4cCI6MTY1ODEyODc5NywiYXVkIjoiaHR0cHM6Ly9rcC1pZGVudG10eXNlcnZlci5henVyZXd1YnNpdGVzLm5ldC9yZXNvdXJjZXMiLCJzY29wZ5I6WyJzdGFmZi10cmFpbmluZy1hcGkiLCJvcGVuaWQiXSwiYW1yIjpbInB3ZCJdLC
JjbGllbnRfaWQiOiJzdGFmZi10cmFpbmluZy13ZWIiLCJzdWIiOiJiNzhkM2YwMi05NzNlLTQ1NTQtOWI5NC04ZTFjYTc1ZTUzOTIiLCJhdXRoX3RpbWUi0jE2NTgxMjUxOTYsImlkcCI6ImxvY2FsIiwiYXR0ZW5kZWVJZCI6IjEwMDA1IiwibGVjdHVyZXJJZ
CI6IjEwMDA0Iiwic2lkIjoiNzQxMkM30DA1MzE50DcwRkEyNTQyODdBN0IwRTEyRkUiLCJqdGki0iI5RUZFQUVEQTA5MzQxNEJDN0NFNzQ0MzI4NkUxNTND0SJ9.nCg5BS8IzkJgmLRUn0rpakgtIy0rGk3tsBkuX0BXTC90J3GTFgwcwtaeWvquiiOr\_m40YUs
pIhP1W0QCQdtgxAPGttKmGPSxZwpRAmIAmzhDh-wkcwWZxx5CDgIibYEf2BZApE\_WiUOqaZ2xTQgcKkPPtxGoqYDAXA9RQnQI9erIdhS9ch6GIEqtS9ID9vgbeLpxS579wWwK11V\_EAuNAHKa60XZqj6oF41XKoVpZEniddsltvN800U\_b1\_b5\_ooh33\_6NCCvlqIAc4mhnAIrOPnddeuySjdvD5gcKns0M-0BK-MLFpNli5IN9zXT6mf\_i-pzbW3ZASap9NVumWHA"

#### **EUVIC:**

#### Metody uwierzytelniania

#### Walidacja tokena



#### API

#### Walidacja tokena

GET /.well-known/openidconfiguration/jwks

CHECK token "exp"

CHECK "alg"

DECRYPTH "signature"

VERIFY IF decrypted

signature equal to:

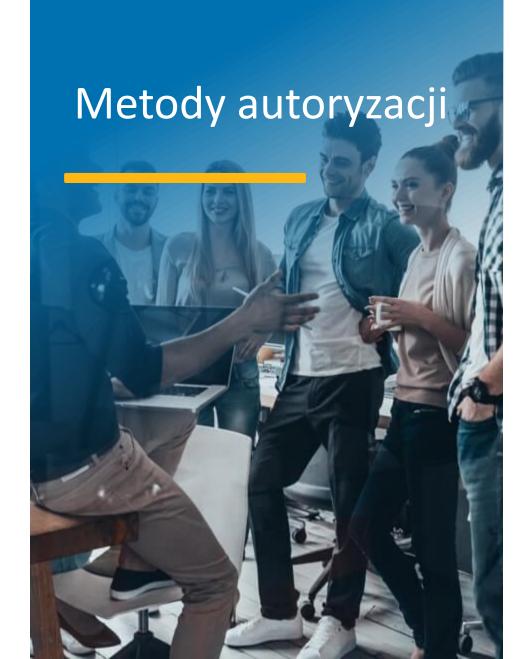
base64UrlEncode(header) + "." + base64UrlEncode(payload)



# A jak zaimplementować walidacje tokena w dotnet core ?

AddAuthentication()✓

AddJwtBearer()✓



# Policy based Authorization

Tworząć policy dla autoryzacji możemy skorzystać z buildera który daje nam następujące możliwości:

- Czy użytkownik jest uwierzytelniony
- Czy uzytkownik ma odpowiednia role w clamie "http://schemas.microsoft.com/ws/2008/06/identity/claims/role"
- Czy użytkownik ma konkretny username
- Czy użytkownik ma claim o konkretnej wartości
- Stworznie customowego requiement



#### Jak to zrobić w kodzie

- Atrybut [Authorize] ✓
- AddAuthorization() ✓
  - PolicyBuilder√
- CustomRequiement√



www.euvic.com