# Bezpieczeństwo usług we współczesnych sieciach

## Bezpieczny dostęp do dokumentów z wykorzystaniem tokenów JWT

---

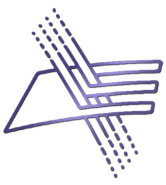
Projekt

Patryk Figiel 325 270

Natalia Topczewska 325 329

---

17 listopada 2025



Wydział Elektroniki i Technik Informacyjnych

POLITECHNIKA WARSZAWSKA

## 1. Opis projektu

Celem projektu jest zaprojektowanie systemu umożliwiającego bezpieczny dostęp do dokumentów z wykorzystaniem tokenów JWT (JSON Web Token). System ten ma realizować kontrolę dostępu do zasobów (dokumentów), weryfikując tożsamość użytkownika przy każdym żądaniu dostępu do dokumentu. Zastosowanie JWT pozwoli na przechowywanie informacji o użytkowniku w tokenie, co sprawi, że serwer nie będzie musiał zarządzać sesjami, a wszystkie dane wymagane do autoryzacji będą zawarte w samym tokenie.

## 2. Budowa JSON Web Tokenów

Token sieciowy JSON (JWT) to bezpieczny sposób przesyłania informacji między klientem a serwerem. Są to dane w postaci JSON'a zabezpieczone podpisem kryptograficznym. Podpis można wykonać przy użyciu następujących metod kryptograficznych:

- HMAC (kod uwierzytelniania wiadomości oparty na haszu)
- RSA lub ECDSA (asymetryczne algorytmy kryptograficzne)

JWT składa się z trzech części rozdzielonych kropkami (.): **Header**, **Payload**, **Signature**.

## 3. Plan realizacji projektu

- **Przegląd bibliotek:** W projekcie planujemy wykorzystanie PyJWT do generowania i weryfikacji tokenów. Rozważamy również alternatywne rozwiązania, takie jak python-jose oraz Authlib, które oferują bardziej rozbudowane funkcje, np. obsługę JWK.
- **Wybór technologii:** Backend systemu będzie oparty na Pythonie, z wykorzystaniem frameworka Flask do budowy API. Na frontendzie zostaną użyte HTML, CSS oraz Next.js do tworzenia interaktywnych aplikacji webowych, które będą współpracować z backendem.
- **Implementacja:** System zostanie zaprojektowany w taki sposób, że po zalogowaniu użytkownik otrzyma token JWT, który będzie przesyłany przy każdym kolejnym żądaniu w nagłówku HTTP. Token ten pozwoli na weryfikację autentyczności użytkownika oraz przydzielenie odpowiednich uprawnień do dostępu do dokumentów.

## 4. Implementacja i wyzwania

- **Stateless Authentication:** Planujemy zastosować podejście stateless, co oznacza, że serwer nie będzie przechowywał sesji użytkowników. Wszystkie dane (np. ID użytkownika, rola) będą zawarte w tokenie JWT, co poprawi skalowalność systemu.
- **Czas wygaśnięcia tokenu:** Zostanie wprowadzony mechanizm, w którym tokeny będą wygasały po 1-2 minutach (na potrzeby prezentacji). Aby zapewnić odpowiedni poziom bezpieczeństwa czas wygaśnięcia tokenu ustawia się zazwyczaj 15 min - 1 h. Po wygaśnięciu użytkownik będzie zmuszony do ponownego zalogowania się lub użycia refresh tokenu do odnowienia sesji.
- **Bezpieczeństwo:** Projekt zakłada użycie HTTPS do bezpiecznego przesyłania danych oraz silnych algorytmów kryptograficznych do podpisywania tokenów, co zapewni integralność i bezpieczeństwo danych.

## 5. Prototyp systemu

Stworzony prototyp systemu ma na celu umożliwienie realizacji logowania użytkowników, generowania tokenów JWT oraz ich weryfikacji podczas próby dostępu do dokumentów. Prototyp pozwoli na przetestowanie kluczowych mechanizmów autoryzacji oraz weryfikacji uprawnień na podstawie roli użytkownika.

## 6. Wnioski i podsumowanie

Dzięki zastosowaniu stateless authentication oraz silnych algorytmów kryptograficznych zapewniamy wysokie standardy bezpieczeństwa, wydajności i skalowalności. Projekt jest w fazie planowania, a po implementacji pozwoli na skuteczną weryfikację użytkowników i kontrolę dostępu do zasobów.