Wyższa Szkoła Ekonomii i Informatyki w Krakowie

Json Web Token

JSON Web Token

- Otwarty standard zabezpieczania komunikacji/informacji
- Zabezpiecza informacje przesyłane w formie JSON
- Przesłane informacje zostają podpisane cyfrowo lub zaszyfrowane
- JWT do podpisywania używa metody sekretnego hasła lub pary kluczy publiczny/prywatny

WSEI

Scenariusze użycia

- Uwierzytelnianie klienta
- Podpisywanie zawartości
- Zapewnienie integralności danych (dane w tokenie)
- Szyfrowanie wiadomości

WSEI

Uwierzytelnianie klienta

- Przesłanie danych do logowania
- Serwer zwraca token

WSEI

Szyfrowanie wiadomości

- Szyfrowanie danych w payload za pomocą klucza publicznego
- Odbiorca weryfikuje token i odszyfrowuje wiadomość za pomocą klucza prywatnego

WSEI

Format tokenu

- Wersja kompaktowa: header.payload.signature
- Header
  Zakodowany w Base64 JSON który zawiera najczęściej typ tokenu (domyślnie JWT) oraz algorytm podpisywania (np. HMAC, SHA256, RSA etc).
- Payload
  Zakodowany w Base64 JSON przechowujący dowolne dane systemu oraz metadane tokena (np. exp - expiration date).
- Signature
  Zakodowany wybranym algorytmem ciąg znaków złożony z nagłówka, danych i sekretnego ciągu znaków (wiem jak to brzmi, no secret po prostu;)).
  Dzięki signature mamy pewność co do integralności zawartych w tokenie informacji

WSEI

Przykładowy token

Online debugger

jwt.io/#debugger-io

WSEI

Przesyłanie tokenu

- Cookie
- Headers (Authorization header - Bearer scheme lub tokeny MAC)
  - Bearer token nie jest szyfrowany, niej jest podpisywany kluczem
- Body

WSEI

Bezpieczeństwo

- Skomplikowany secret
- Generowanie tokenów z secret opartym na metadanych użytkownika
- Krótki czas życia tokenu (dostosowany do systemu - np. 1h, 1d)
- Krótki czas życia tokenu v2 - np. 5min oraz mechanizm refresh/revoke token
- Szyfrowany token może być pojemnikiem na wrażliwe dane sesyjne (zamiast sessionStorage/ localStorage/cookies/localDB)

WSEI

Wyższa Szkoła Ekonomii
i Informatyki w Krakowie