Tokeny JWT

Czyli o uprawnieniach słów kilka

Grębowski Łukasz

2019

# Tokeny JWT

JWT – Json Web Token jest otwartym standardem (RFC 7519) tworzenia tokenów dostępowych, które zawierają w sobie pewną porcję danych (payload). Siłą tokenów jest to, że mogą przenosić dowolną porcję danych i informacji o użytkowniku. Token składa się z trzech części:

Nagłówka – określa jaki algorytm szyfrowania został wykorzystany do utworzenia podpisu tokena.  
Payloadu – tu znajdują się dekodowane w base64 uprawnienia/informacje przenoszone w tokenie.  
Podpisu cyfrowego – podpis payloadu token-a. Podpisany kluczem prywatnym serwera (dostawcy token-a). Zabezpiecza token przed modyfikacją.

Należy zaznaczyć iż domyślnie tokeny JWT nie posiadają funkcji pozwalających na wykluczenie przechwycenia tokena. Często w tokenach umieszcza się takie informacje jak ip, rodzaj przeglądarki (user-agent). Tokeny mają różne czasy życia, w przypadku aplikacji o wysokich wymaganiach bezpieczeństwa tokeny z pozwoleniami np. przelewu mogą być jednorazowe.

Uwaga! Użycie tokenów nie eliminuje konieczności użycia rozwiązań pozwalających zachować poufność przesyłanych informacji. Nie należy rozumieć tokenów JWT jako rozwiązań tej klasy co np. SSL.

Token przesyłany jest w nagłówku „Authorization” zapytania HTTP.

# Wykorzystanie JWT w aplikacji Pubweb

Rolą JWT w aplikacji Pubweb jest wykluczenie konieczności każdorazowego logowania loginem i hasłem oraz możliwość przekazywania informacji pomiędzy serwisami takich jak role i przywileje w spójnej formie. Użycie tokenów JWT pozwala również na ograniczenie konieczności odpytywania punktu autoryzacyjnego o dane użytkownika za każdym razem.

Standardowy schemat autoryzacji przy pomocy tokena JWT wygląda następująco:

1. Użytkownik wysyła hasło i login do serwera autoryzacyjnego
2. Serwer autoryzacyjny zwraca token JWT wraz z informacjami o tym jakie uprawnienia posiada użytkownik w aplikacji, do podpisu JWT użyty jest klucz prywatny serwera autoryzacyjnego
3. Użytkownik używa tokenu wygenerowanego przez centrum autoryzacji do wykonania operacji, w którymś z mikroserwisów.
4. Mikroserwis udziela lub nie udziela zgody na wykonanie operacji na podstawie:

4.1. Sprawdzenia za pomocą klucza publicznego serwera autoryzacji autentyczności JWT (porównanie podpisów).

4.2. W przypadku, gdy weryfikacja z 4.1. przebiegła pomyślnie serwis sprawdza czy w JWT zawarte są uprawnienia (np. Role/przywileje) wymagane do wykonania danej operacji

4.3. Mikroserwis wykonuje inne walidacje biznesowe charakterystyczne dla danej operacji

Powyższy schemat ma poniższe implikacje:  
- Jeżeli dojdzie do rozszerzenia uprawnień użytkownika to po stronie użytkownika leży wygenerowanie i używanie nowego tokena o adekwatnych uprawnieniach

- Jeżeli dojdzie do ograniczenia uprawnień użytkownika to z punktu widzenia autoryzacji za pomocą JWT wejdzie ono w życie dopiero po wygaśnięciu poprzedniego tokena. Dla operacji o wysokim stopniu bezpieczeństwa potrzebny jest dodatkowy mechanizm autoryzacji (np. każdorazowe odpytywanie serwera autoryzacyjnego o uprawnienia użytkownika, którego dotyczy JWT).