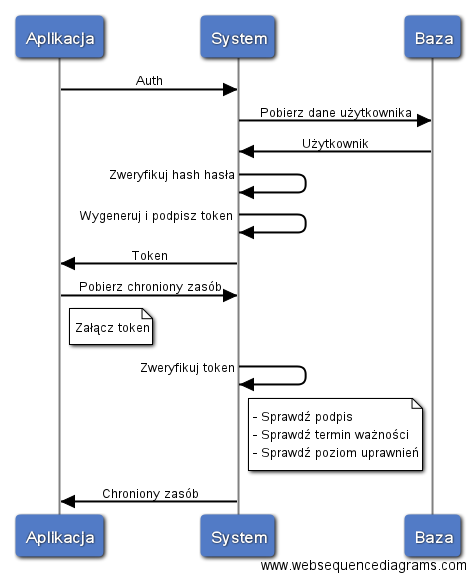
Dostęp do chronionych zasobów systemu oparty jest autentykację z wykorzystaniem technologii JSON Web Tokens (JWT) opisanej w standardzie RFC7519 (<https://tools.ietf.org/html/rfc7519>). JWT wykorzystuje tak zwane tokeny, czyli ciągi znaków identyfikujących sesję i potwierdzających prawa posiadacza tokenu (aplikacji klienta) do dostępu do żądanych zasobów. Zaletą technologii JWT jest:

* Bezstanowość – informacje o sesji zawarte są w samym tokenie i nie jest wymagane przechowywanie ich po stronie serwera. Eliminuje to problem zarządzania cyklem życia sesji i usuwania wygasłych sesji.
* Bezpieczeństwo – każdy token podpisany jest kluczem kryptograficznym, w tym wypadku bezpiecznym algorytmem HS256.
* Łatwość implementacji – informacje zawarte w tokenie są zwięzłe i oparte o czytelny format JSON.

Typowy przebieg działania aplikacji, która wymaga dostępu do chronionego zasobu systemu, przedstawia poniższy diagram.



Symulacja scenariusza z użyciem komendy curl:

1. Aplikacja wywołuje końcówkę /auth metodą POST, przekazując nazwę użytkownika i hasło w formacie JSON zawartym w treści żądania:

curl -X POST -H "Content-Type: application/json" -d '{"username": "admin", "password" : "abc123"}' <http://192.168.56.2:8080/auth>

1. System, po pozytywnej weryfikacji nazwy użytkownika i hasła zwraca wygenerowany token:

{

"access\_token": "eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VybmFtZSI6ImFkbWluIiwicm9sZSI6IkdMT0JBTF9BRE1JTiIsImV4cCI6MTQ3ODI4NjAyNCwiaWF0IjoxNDc4MTk5NjI0LCJuYmYiOjE0NzgxOTk2MjQsImlkZW50aXR5IjoiYWRtaW4ifQ.IVOIGDt4o9ksMKguZMzLVeRhr5Y\_aYxuPMPHtb2HbY8"

}

Token ten zawiera następujące informacje zakodowane w formacie BASE64:

Nagłówek  
{  
 "alg": "HS256",

"typ": "JWT"

}

Dane

{

"username": "admin",

"role": "GLOBAL\_ADMIN",

"exp": 1478286024,

"iat": 1478199624,

"nbf": 1478199624,

"identity": "admin"

}  
Ostatnią część stanowi podpis kryptograficzny.

1. Aplikacja wysyła żądanie do docelowego zasobu, dodając nagłówek *Authorization* zawierający słowo „JWT” i otrzymany token:

curl -X GET -H 'Authorization: JWT eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VybmFtZSI6ImFkbWluIiwicm9sZSI6IkdMT0JBTF9BRE1JTiIsImV4cCI6MTQ3ODI4NjAyNCwiaWF0IjoxNDc4MTk5NjI0LCJuYmYiOjE0NzgxOTk2MjQsImlkZW50aXR5IjoiYWRtaW4ifQ.IVOIGDt4o9ksMKguZMzLVeRhr5Y\_aYxuPMPHtb2HbY8' http://192.168.56.2:8080/api/v1/users/