JWT (Json Web Token)

Um padrão que define uma maneira compacta, auto-contida de transmitir informações de maneira segura entre duas partes através de um objeto JSON.

Estrutura do JWT

Formado por 3 secções separados por pontos:

1. **Header:** contem informações da geração do token;
2. **Payload:** contem claims (informações) sobre a entidade (normalmente dados do usuário autenticado) e outras informações adicionais.

   Estas claims (informações) podem ser de 3 tipos:

   a) ***Registered Claims***: Não obrigatórios, mas recomendados utilizados no momento da validação do token;
   Ex: sub(subject), iss(issuer), exp(expiration), iat(issued at), aud(audience).

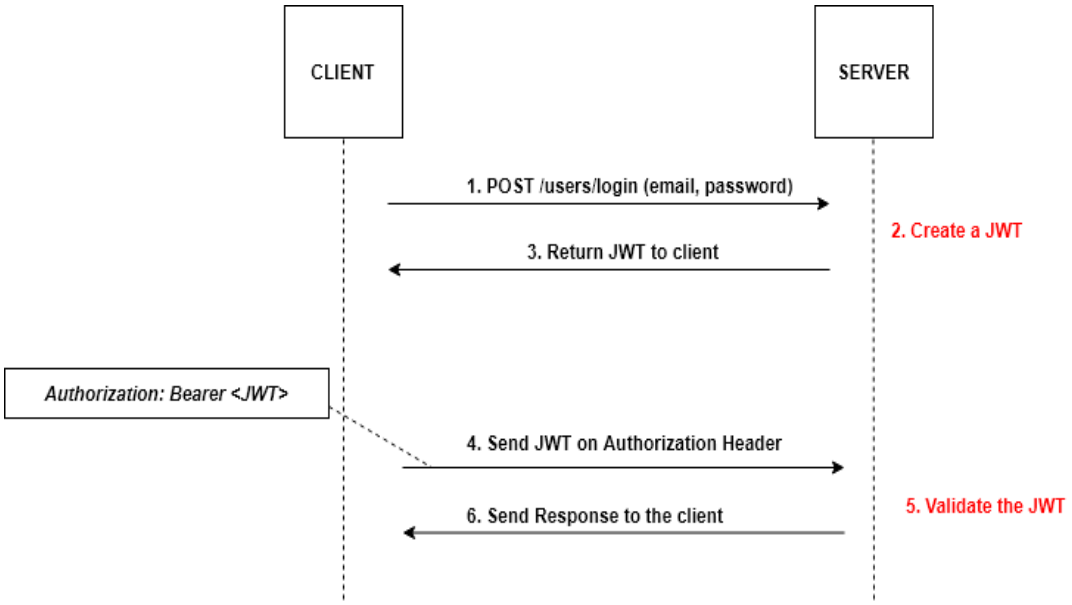
   b) ***Public Claims:*** Informações utilizados na aplicação podendo ser dados do usuário autenticado.

   c) ***Private Claims:*** atributos utilizados normalmente para partilhar informações entre aplicações.

3. **Assinatura:** gerado apartir da juncão do hash do ***HEADER*** e do ***PAYLOAD*** *utilizando a função* ***base64UrlEncode*** e uma chave secreta da aplicação.

Utilização do JWT no cenário de uma API RESTful

Apos se fazer o login em um recurso de autenticação na API um token deve ser criado e retornado ao cliente normalmente no cabeçalho. Este token retornado deverá ser utilizado nas próximas requisições pelo cliente para o acesso a recursos protegidos.



Link uteis

https://jwt.io/

https://jwt.io/introduction/

https://tools.ietf.org/html/rfc7519#section-4.1