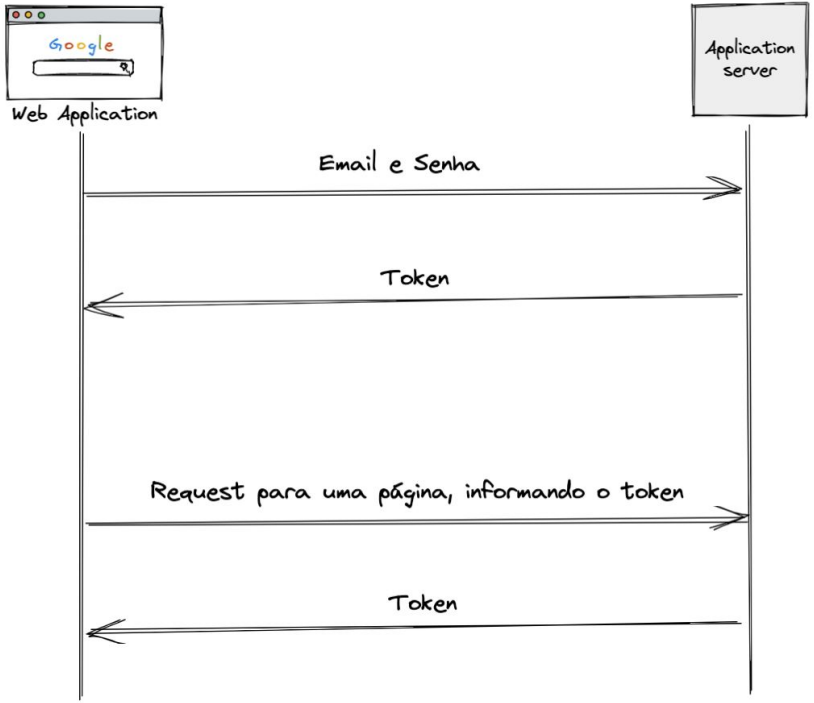
Introdução

Nesse módulo estudamos sobre como podemos deixar nossas aplicações seguras ao autenticar os usuários que utilizam APIs.

Autenticação

Quando falamos de APIs, a autenticação de usuários é feita por meio de tokens de acesso.

Tokens são como credenciais que são geradas quando uma pessoa submete suas informações de autenticação corretamente para um fluxo de autenticação, como email e senha, por exemplo.



Uma vez que as credenciais são informadas corretamente, a aplicação web retorna um token que deve ser enviado em todas as futuras requisições em endpoints autenticados.

Spring Security

O **Spring Security** é o framework de segurança padrão para aplicações **Spring**. Permite aos desenvolvedores configurarem de maneira muito customizada autenticação e controle de acesso em aplicações web e **APIs** baseadas no **Spring**.

- Documentação: https://spring.io/projects/spring-security

OAuth

OAuth é um framework de autorização que permite aplicações obterem acesso limitado a contas de usuários através de um serviço HTTP, como por exemplo Facebook, GitHub, Google, etc...

Funciona delegando a autenticação de usuário para o serviço que contém a conta do usuário em si, permitindo que o serviço responsável pela conta possa autorizar outras aplicações a acessar esses dados.

Exemplo de uma aplicação que permite fazer login usando o OAuth.
Especificação do padrão OAuth: https://oauth.net/2/

JWT (JSON Web Token)

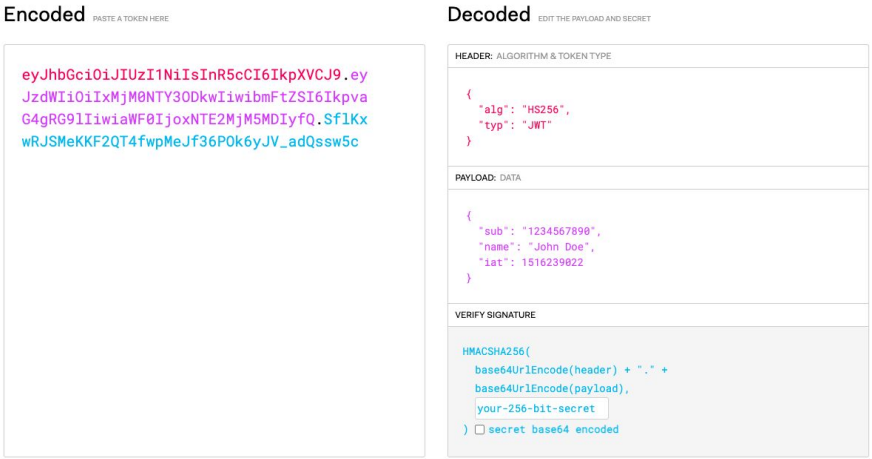
O **JWT** é um padrão aberto que define uma maneira compacta e auto contida de transmitir informações nas requests através de objetos **JSON**.

Essas informações podem ser verificadas e consideradas verdadeiras porque o token é assinado digitalmente. Eles podem ser assinados utilizando um segredo com um algoritmo **HMAC** (https://pt.wikipedia.org/wiki/HMAC) ou utilizando um par de chaves pública/privada, como **RSA** (https://pt.wikipedia.org/wiki/RSA_(sistema_criptogr%C3%A1fico)) ou **ECDSA** (https://pt.wikipedia.org/wiki/ECDSA)

Exemplo de um token JWT:

```
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJzdWIiOiIxMjM0NTY3ODkwIiwibmFtZSI6IkpvaG4gRG9lIiwiaWF0IjoxNTE2MjM5MDIyfQ.SflKxwRJSMeKKF2QT4fwpMeJf36POk6yJV_adQssw5c
```

Os tokens **JWT** são divididos em **três partes**: cabeçalho (**header**, em `verde`), corpo (**payload**, em `vermelho`) e assinatura de verificação (**verify signature**, em `azul`).



É possível aprender mais sobre JWT no site oficial: https://jwt.io/

Keycloak

O **Keycloak** é um servidor de de gerenciamento de autenticação e autorização de código aberto administrado pela **Red Hat**, desenvolvido em Java.

O **Keycloak** implementa e disponibiliza funcionalidades comuns e completas usadas para gerenciamento de contas de usuários, sendo ideal para pequenos ou grandes projetos. Dentre as funcionalidades, há:

- Criação de usuários
- Login
- Recuperação de senha
- Ativação de usuário por meio de confirmação de email
- Necessidade de aceitação de termos de uso
- Personalização de páginas de cadastro e login
- Gerenciamento de permissões
- Gerenciamento de grupos de usuários
- Internacionalização (i18n)

Site do Keycloak: https://www.keycloak.org/