Parte A - contexto

Autenticação em serviços

1. basic HTTP-based authentication
2. API Keys & Tokens
3. HMAC
4. OAuth 2.0
5. OpenID Connect

ver por exemplo esta descrição.

API Key

- usualmente associadas a um dispositivo ou aplicação, e usadas como parâmetro numa operação
- tem a ver com a origem de um pedido
- podem transmitir-se:
  - no header do pedido HTTP (base ou custom header)
  - no corpo do pedido HTTP
  - *query parameter* posterior ao caminho do pedido (path?key=WJDHRU543sx)

API Token

- representam credenciais de segurança sobre uma entidade
- podem ter campos (*Header*, *Payload*, e *Signature* - uma forma de assinatura)
- está relacionado com o utilizador particular de um pedido, e dos seus respetivos direitos
- mais relevantes se for necessária uma autorização a dados por utilizador
- podem ter validade, curta

Visualmente, são apenas sequências de caracteres que se transmitem com algum pedido. É comum a confusão entre ambos os termos.

Em geral, estes conceitos são empregues consecutivamente: primeiro as chaves, depois as tokens (exemplo para os serviços twilio).

Parte B - exercício com JWT

1. Vamos testar o projeto
Token-based API authentication with Spring and JWT.

Obtenha o código inicial daqui.

2. Analise código fonte.

Note-se que o importante é entender o uso do token JWT

- como foi gerado
- como é enviado
- o que contém
- o que o serviço protegido faz para validar a autorização de acesso

A ideia é testar o uso de Tokens.
A parte de autenticação não está tratada em profundidade. No caso ela é simulada no mesmo servidor, apenas para simplificar.

3. testar um pedido

- no browser (http://localhost:8080/hello)
- e via curl

```
$ curl http://localhost:8080/hello
```

Espera-se uma resposta semelhante a:

```
{"timestamp":"2022-12-09T12:49:39.258+0000","status":403,"error":"Forbidden","message":"Access Denied","path":"/hello"}
```

4. Gerar um Token

O token será obtido do "servidor de autenticação" simulado:

http://localhost:8080/user

com post de user e password, como no HTML de exemplo, no ficheiro ao lado.

O Token é devolvido após "a autenticação simulada"...

5. testar o decode do token:

https://jwt.io/

6. Usar o token para acesso autenticado à API do serviço.
Vamos aplicar o Token num HTTP Header, "Authorization".

Exemplo (mas lembre-se de atualizar o valor do token - Não faça Copy-paste!)

```
$ curl -H 'Authorization: Bearer eyJhbGciOiJICvojsNLnCbq1xQgZUmrkEg' http://localhost:8080/hello
```

Nota: esta experiência usa o código do projeto descrito neste apontador.
O código simplifica (demasiado) a parte da autenticação.
E tem um parâmetro secreto em dois locais do código fonte, quando deveria ter a leitura desse valor desde um ficheiro de configurações.