

# Desenvolvimento de Componentes Distribuídos API

Leandro Duarte Pulgatti

2021

## 1 Descrição da tarefa

Pesquise e escreva um texto sobre a API de autorização chamada OAuth.

1. Para que serve e para o que foi criado o protocolo OAuth? Utilize de imagens e exemplos.

**R:** Protocolo OAuth é uma camada de autenticação entre uma aplicação terceira(client), a proprietária dos recursos (resource owner) e o controlador desses recursos (resource server), onde o usuário consente a liberação de acesso a alguns dados limitados, dados esses contidos no controlador dos recursos citados acima. O protocolo OAuth foi criado para garantir segurança no tráfego das informações entre as aplicações, pois o usuário está consentindo o acesso entre elas; O protocolo OAuth também permite que aplicações terceiras tenham acesso a dados necessários para eles, sem precisar de dados específicos ou muito importantes para o usuário, como dados de login.

O protocolo OAuth segue o seguinte modelo:

### Fluxo Abstrato do Protocolo



2. Descreva o fluxo do protocolo OAuth na versão 2.0" Quais os agentes envolvidos?

Qual o fluxo de informação entre estes agentes?

**R:** Os agentes envolvidos são o proprietário dos recursos, o cliente, o servidor de recursos e o servidor de autorização, proprietário de recurso sendo o usuário e é quem autoriza a aplicação a acessar sua conta, já servidor de recurso e de autorização podem ser vistos como API e podem ser combinados, servidor de recurso hospedando as contas de usuário protegidas e o servidor de autorização verificando a identidade do usuário para então emitir tokens de acesso para a aplicação, por último, o cliente será a aplicação que é quem quer acessar a conta do usuário, mas antes disso deve ser autorizada por ele, e essa autorização validada pela API.

Como já demonstrado na questão 1, não é necessário novamente colocar a imagem, mas irei explicar qual é o fluxo do diagrama representado na imagem: primeiramente a aplicação solicita a autorização para acessar os recursos do serviço do usuário, caso o usuário autorize a solicitação, a aplicação recebe a concessão de autorização, a aplicação então solicita um token de acesso ao servidor de autorização (API) através da autenticação de sua própria identidade, e da concessão de autorização, se a identidade da aplicação estiver autenticada e a concessão de autorização válida, o servidor de autorização irá emitir um token de acesso para a aplicação, assim a autorização estará completa, como a aplicação já possui a autorização, agora ela solicita recurso ao servidor de recurso (API) apresentando seu token de acesso para ser autenticado, se o token de acesso for válido, o servidor de recurso fornecerá o recurso que a aplicação pede. O fluxo poderá mudar dependendo da concessão dada, mas ideia de fluxo de como OAuth funciona é sempre parecida.

3. Descreva como este serviço, se mal utilizado, pode trazer problemas de segurança para uma empresa.

**R:** Caso não seja configurado da forma correta, o OAuth abre margem para ataques pois fica vulnerável em pontos importantes, ao invés de ter como grande ponto forte a segurança dos dados, se mal configurado, acaba dando livre acesso para pessoas mal intencionadas que queiram roubar informações.

4. Cite pelo menos 10 serviços, de grandes empresas provedoras de autorização que utilizam, este protocolo.

**R:** Empresas conhecidas que utilizam esses sistemas são Google, Twitter, Facebook, GitHub, Spotify, VK, Apple, Netflix, Paypal e Microsoft, existem varias outras, mas entraria em redundância cita-las pois são do mesmo ramo das empresas citadas acima.

LEMBRE-SE, este material deve ser original, leia e escreva "com suas palavras" o que entendeu sobre o assunto. Utilize exemplos e figuras para demonstrar seu conhecimento, elas ajudam a entender o que está sendo escrito.

Quanto mais completa for sua resposta, mais completa será sua nota.

## 2 Sobre o trabalho

### Individual

**Método de entrega:** envie um arquivo no formato PDF para o e-mail leandropulgatti@uniopet.edu.br

**Nome do arquivo:** DISTRIBUIDO\_1\_<NOME> <MATRÍCULA>

**Título do e-mail:** a mesma regra do nome do arquivo. **Prazo:** 19:00:00 horas do dia 16/03/2021

## 3 Demais Regras

- Os trabalhos são individuais.
- Os trabalhos não serão aceitos após a data/hora limite.
- Caso o e-mail com o trabalho seja enviado mais de uma vez, somente o último e-mail enviado será considerado;
- Qualquer indício de cópia de qualquer fonte resultará na perda total dos pontos do trabalho.

## 4 referencias

- <https://tools.ietf.org/html/rfc6749>
- <https://oauth.net>