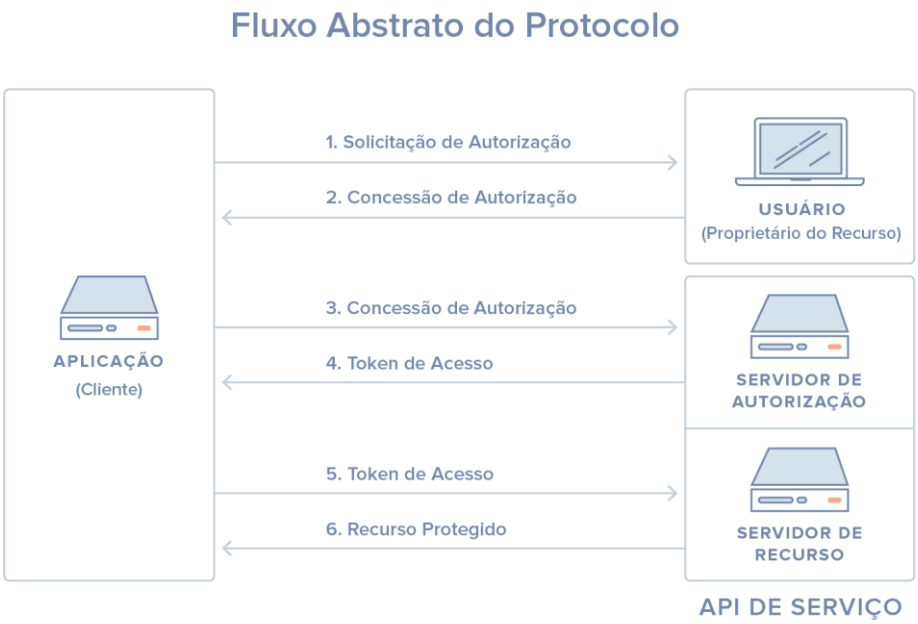
**1 – Para que serve e para o que foi criado o protocolo OAuth? Utilize de imagens e exemplos.**

O protocolo OAuth é chamado quando há uma interação “client” com a API. Permite ao usuário acesso limitado a recursos de uma website sem expor seus dados, também é de interações com os dados do usuário como “Login e senha”, criada afim de manter a segurança de acesso a recursos de terceiros. Podemos citar como exemplo o carro próprio, que damos a nossa chave ao manobrista para estacionar, porem ele não irá dirigir por muitos metros, então daríamos a chave especial, o que lhe dará permissões limitadas ao carro.

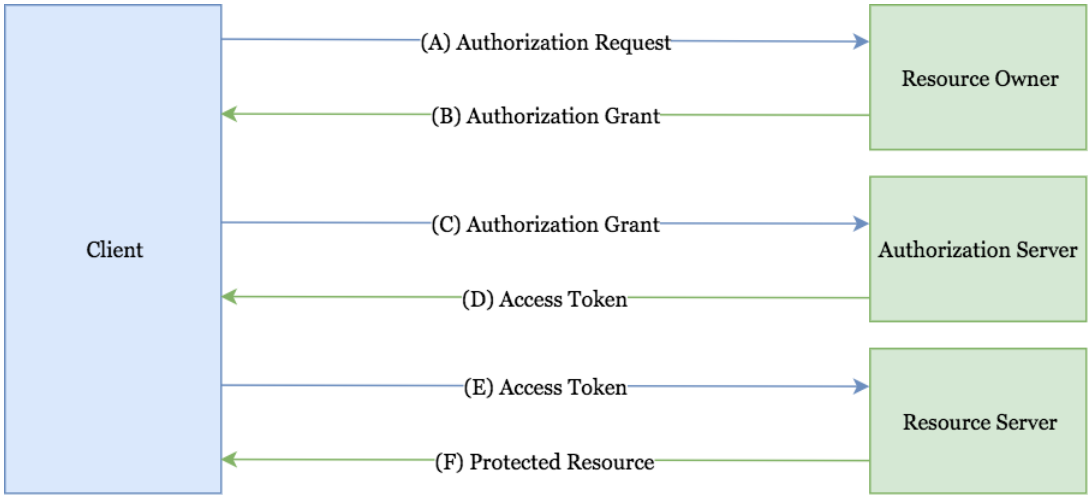



**2 – Descreva o fluxo do protocolo OAuth na versão 2.0”**

- **Quais os agentes envolvidos?**
  - Resource Owner: Entidade que controla o acesso aos recursos protegidos(proprietário de recursos);
  - Resource Server: Hospeda os recursos a serem acessados e recebe requisições (servidor que sede os recursos);
  - Authorization Server: Gera tokens de acesso, o que permite o Client acesse os recursos (servidor de autorização);
  - Client: que solicita tokens ao Authorization Server, para ter acesso a recursos protegidos do Resource Owner(aplicação).
- **Qual o fluxo de informação entre estes agentes?**

  O Client pede autorização (Authorization request) ao Resource Owner para acessar seus recursos, então o Client recebe um concessão de autorização (Authorization Grant), após isso o Client solicita um token de acesso (access token) ao Authorization Server, enviando o Authorization Grant. Com tudo bem sucedido o Client pede acesso aos recursos ao Resource Server, se autenticando com o access token. Assumindo que

a validez do access token, o Resource Server responde a requisição do Client com o recurso protegido (Protected Resource).




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

No protocolo OAuth temos a concessão de autorização implícita (Authorization Grant Implicit), em que o fluxo é o mais simplificado possível, sendo o mais inseguro. Por que em vez de receber o Authorization Code(código de autorização) para pedir o access token, é recebido o access token diretamente pelo URI de redirecionamento que vai providenciar na requisição. Nesse método nenhuma credencial intermediaria é emitida, expondo facilmente o access token, que pode acabar vazando informações da empresa.

4 – Cite pelo menos 10 serviços, de grandes empresa provedoras de autorização que utilizam esse protocolo.

- 1 – Amazon: trabalha com e-commerce, computação em nuvem, digital streaming e inteligência artificial;
- 2 – Apple: trabalha com sistema que possibilita aos usuários criarem suas contas para serviços de terceiros com o mínimo de informações pessoais;
- 3 – DailyMotion: trabalha com tecnologia de compartilhamento de vídeos;
- 4 – Discord: trabalha com mensagem instantânea e distribuição digital projetada para criação de comunidades;
- 5 -GitHub: provedor de hospedagem na Internet para desenvolvimento de software e controle da versão usando Git;
- 6 – Google: trabalha com serviços e produtos relacionados a internet, que incluem tecnologias de publicidade online;
- 7 – Instagram: serviço de rede social de compartilhamento de fotos e vídeos de propriedade do Facebook;

- 8 – Netflix: é uma plataforma de conteúdos e empresa de produção over the top;
- 9 – Paypal: plataforma que opera sobre sistema de pagamento e transferência eletrônica de dinheiro online;
- 10 – Vimeo: plataforma de hospedagem e compartilhamento de vídeos, concentra-se na entrega de vídeos de alta qualidade;