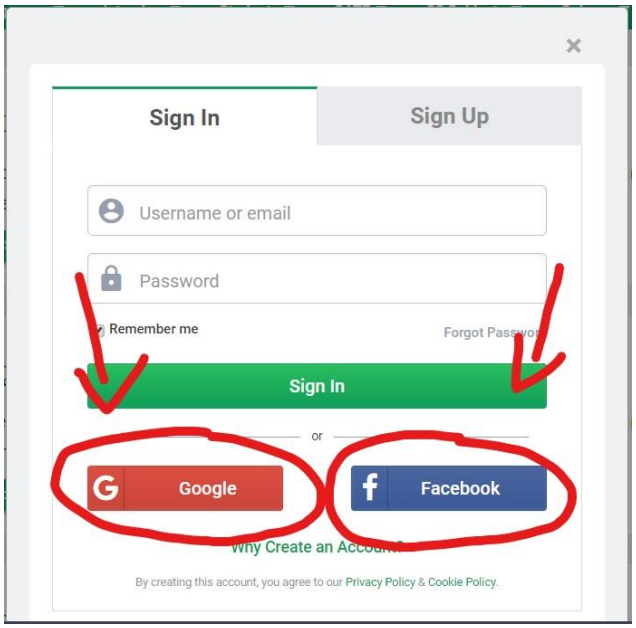
Desenvolvimento de Componentes Distribuídos

API

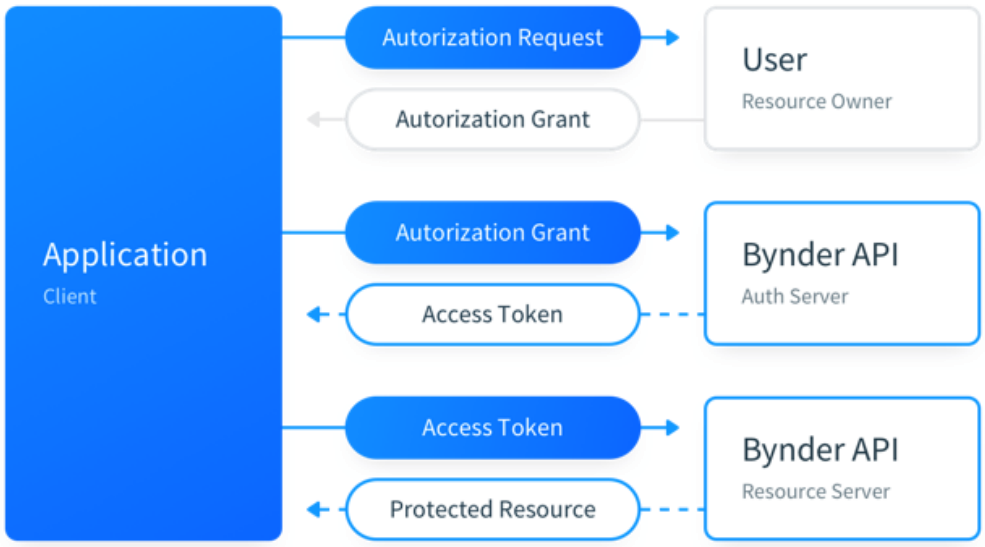
OAuth:

O OAuth nada mais é do que um SSO (Single Sign-On) usado para permitir que as pessoas possam “logar” de uma forma segura em sites utilizando suas contas do Google, Facebook, Apple e etc, por exemplo.



O OAuth 2.0, por outro lado, passa a ser um tipo de protocolo feito para que a pessoa que está navegando por um site tenha consiga ter um acesso limitado sem que suas informações sejam expostas. O OAuth 2.0 possuí os seguintes agentes:

- **Resource Owner (Dono do Recurso):** Ente que tem controle dos recursos protegidos.
- **Resource Server (Servidor do Recurso):** Servidor que receberá as requisições e que abriga os recursos protegidos.
- **Client (Cliente):** É a aplicação que pedirá o acesso aos recursos que são protegidos pelo Resource Owner (Dono do Recurso).
- **Authorization Server (Servidor de Autorização):** É o servidor que após autenticar e receber autorização, vai dar um token de acesso ao Client.



A mal utilização pode acabar gerando vulnerabilidades prejudiciais, tais como o vazamento do Token de acesso pela URL da página ou até mesmo pelo histórico de navegação, por exemplo. Outro exemplo seria a “injeção” do Token, que basicamente significa que podem utilizar um Token vazado ou roubado para se passar pelo Resource Owner quando o Client aceitar o Token de acesso.

Alguns exemplos de grandes Empresas que utilizam tal protocolo seriam:

- Amazon
- DropBox
- GitHub
- Apple
- Discord
- Netflix
- Facebook
- Instagram
- Twitch
- Reddit