Autenticação vai ser utilizado OAuth2  
Existem vários tipos de API.

Aplication Program Interface

API – Não guardamos estados, como sessão. Porque ela pode ser consumida por qualquer outra aplicação externa, ela fica aberta.

Problemas em uma API

* Segurança
* Aplicação distribuídas
* API Externas
* Autenticação de usuários
* Autenticação de clientes

APIS do Google, Facebook – São abertas.

Quando desenvolver uma API temos que pensar na “AUTENTICAÇÃO E SEGURANÇA”.

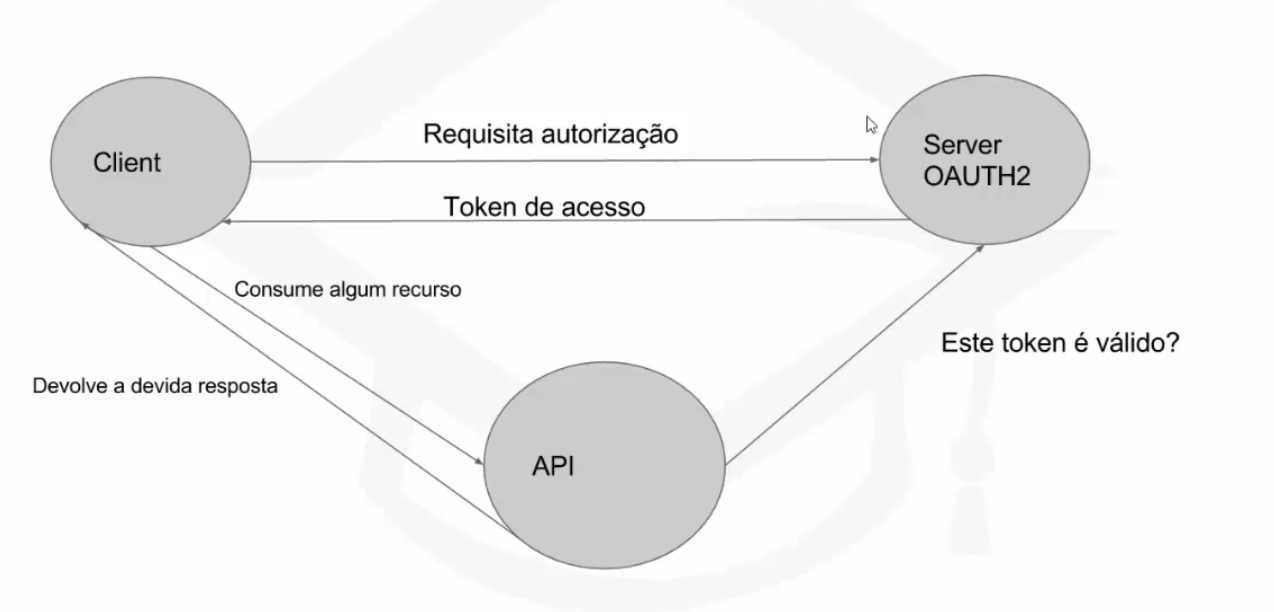
O Que é OAUTH2?

* Protocolo de comunicação
* Permite acesso de aplicação e API externas
* Toda aplicação e API externas é um cliente
* Todo cliente tem acesso limitado ao método HTTP
* Todo acesso é feito via um token de acesso

Segundo a especificação do IETF (RFC 6749):

* Resource Owner: o usuário
* Resource Server:a API
* Authorization Server: quase sempre o mesmo que o servidor da API
* Client: os aplicativos de terceiros

Como é na Prática?



Mais Detalhes do OAUTH2

* O token de acesso tem seu tempo de vida
* O token de acesso pode ser renovado (Refresh token)
* O token de acesso pode ser destruído (Revoke)
* <https://tools.ietf.org/html/rfc6749>

Segurança Com OAUTH2

* Exposição do token
* Qualquer pessoa pode interceptar o token
* Token deve ser passado header da requisição HTTP
* Devemos usa HTTPS/SSL