I DON'T CARE ABOUT SECURITY

(AND NEITHER SHOULD YOU)

I DON'T CARE ABOUT SECURITY

(AND NEITHER SHOULD YOU)

ABOUT ME

Bruno Krebs

Twitter: @brunoskrebs

GitHub: /brunokrebs

Auth0

R&D Content Architect

QUAL O PROBLEMA?

@brunoskrebs

EU POSSO FAZER HASHING E SALTING

@brunoskrebs

Milhões de senhas de Faceboo

https://www.tecmundo.com.br/redes-sociais/139743-senhas-contas-facebook-i...

Apps | blog | rest-flex | auth0 | languages | tools

BUSCAR

tecmundo

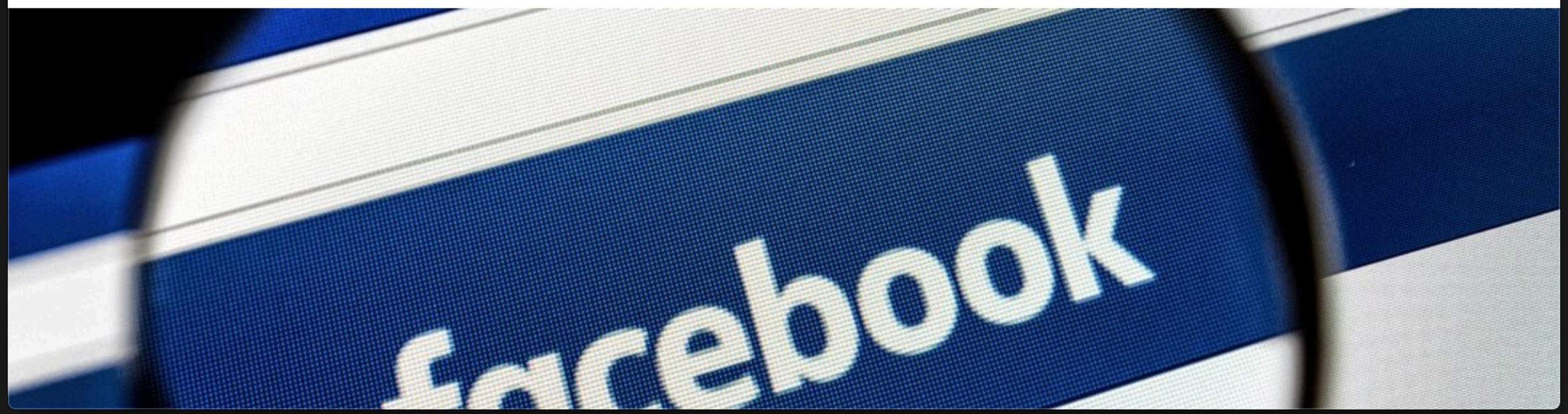
Curtir 6,2 mi

NOTÍCIAS | COMPARAR CELULARES | CUPONS DE DESCONTO | VOXEL | TECMUNDO TV | TECMUNDO DESCONTOS

Milhões de senhas de Facebook e Instagram ficaram expostas funcionários

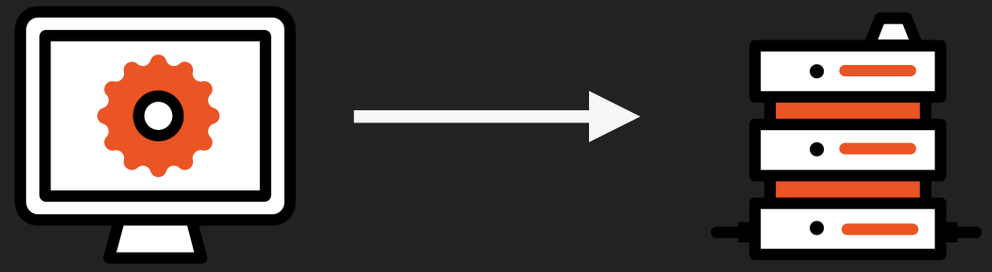
POR **DOUGLAS CIRIACO** | @dciriaco - EM **REDES SOCIAIS** - 21 MAR 2019 — 14H52

COMPARTILHAR | 8 | **234** compartilhamentos



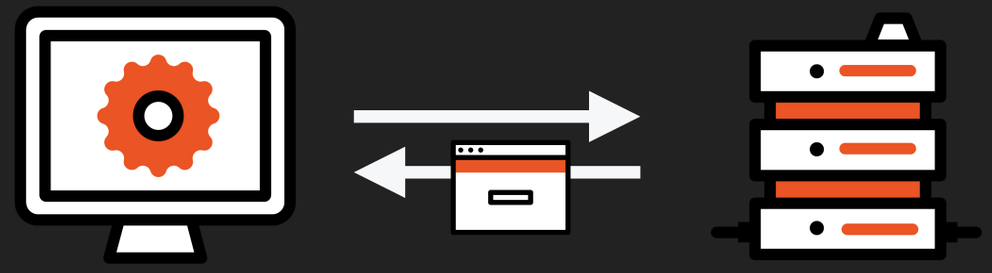
APLICAÇÕES TRADICIONAIS

- Browser acessa página de login



APLICAÇÕES TRADICIONAIS

- Browser acessa página de login

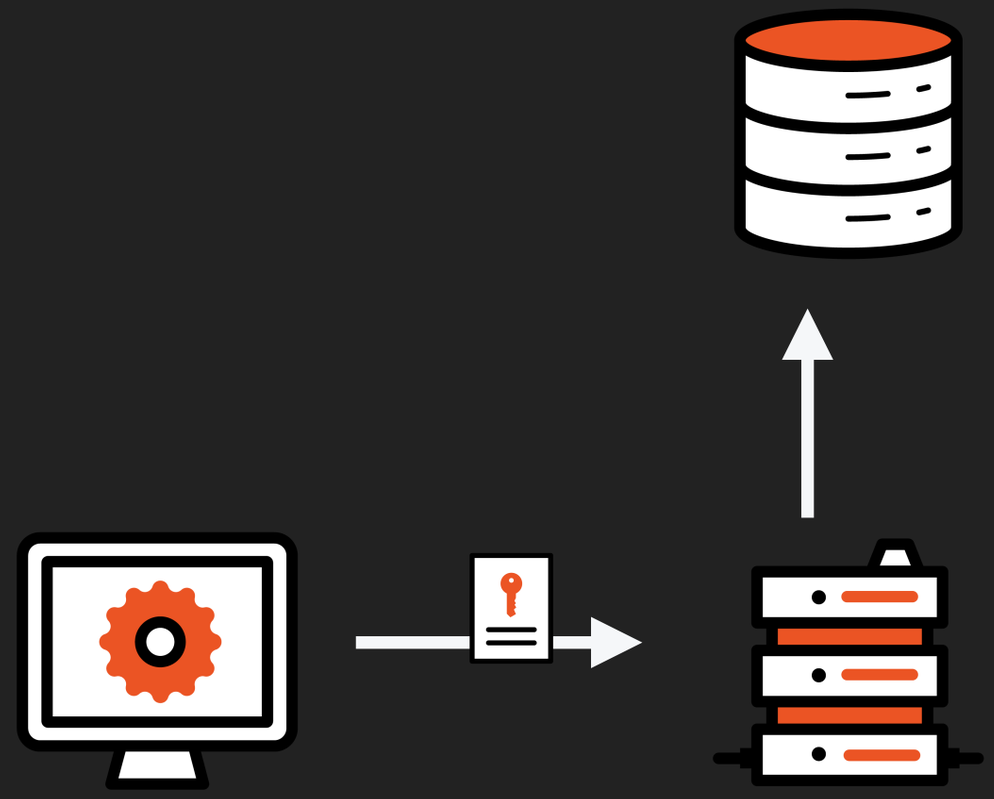


APLICAÇÕES TRADICIONAIS

- Browser acessa página de login

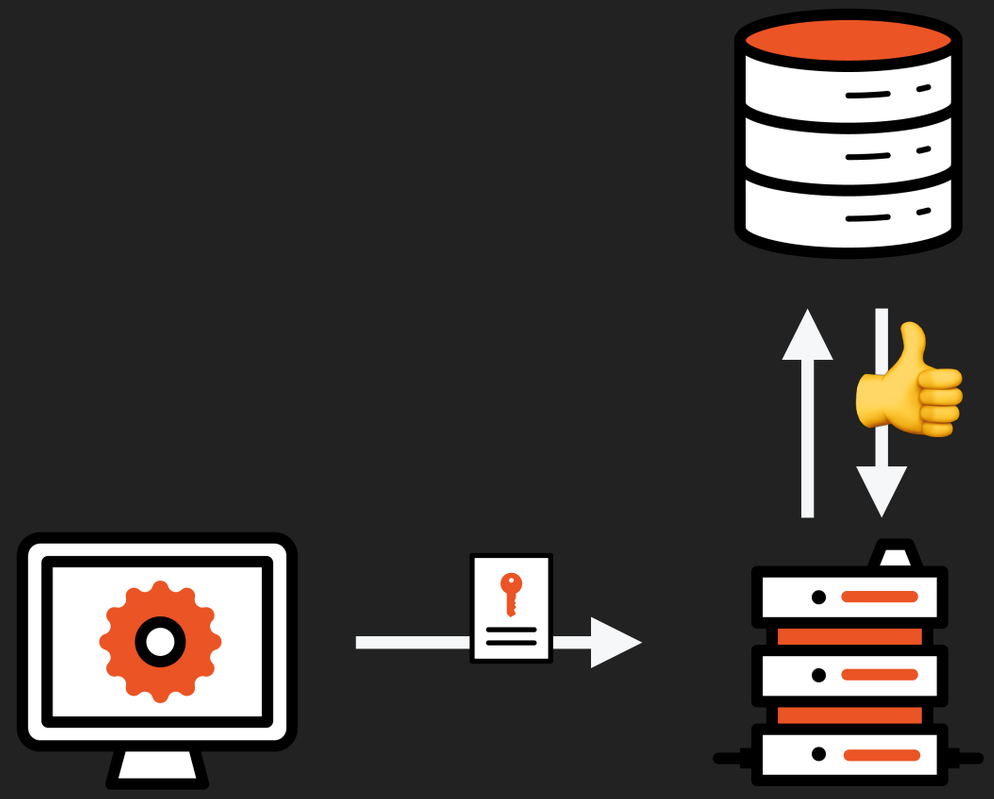
APLICAÇÕES TRADICIONAIS

- Browser acessa página de login
- Servidor valida as credenciais



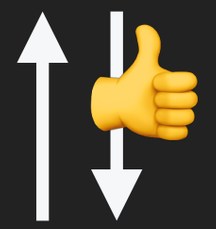
APLICAÇÕES TRADICIONAIS

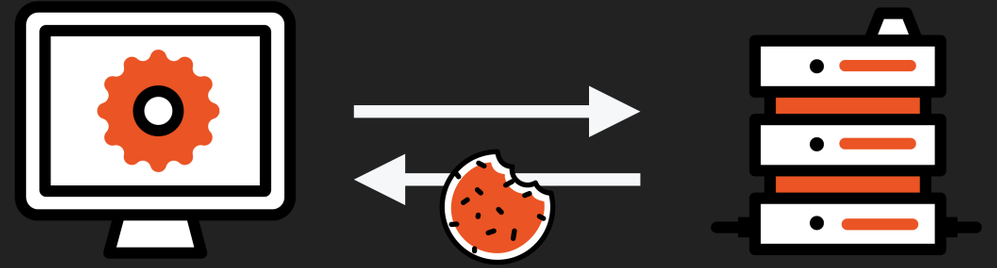
- Browser acessa página de login
- Servidor valida as credenciais



APLICAÇÕES TRADICIONAIS

- Browser acessa página de login
- Servidor valida as credenciais
- Uma sessão é estabelecida e um cookie gerado



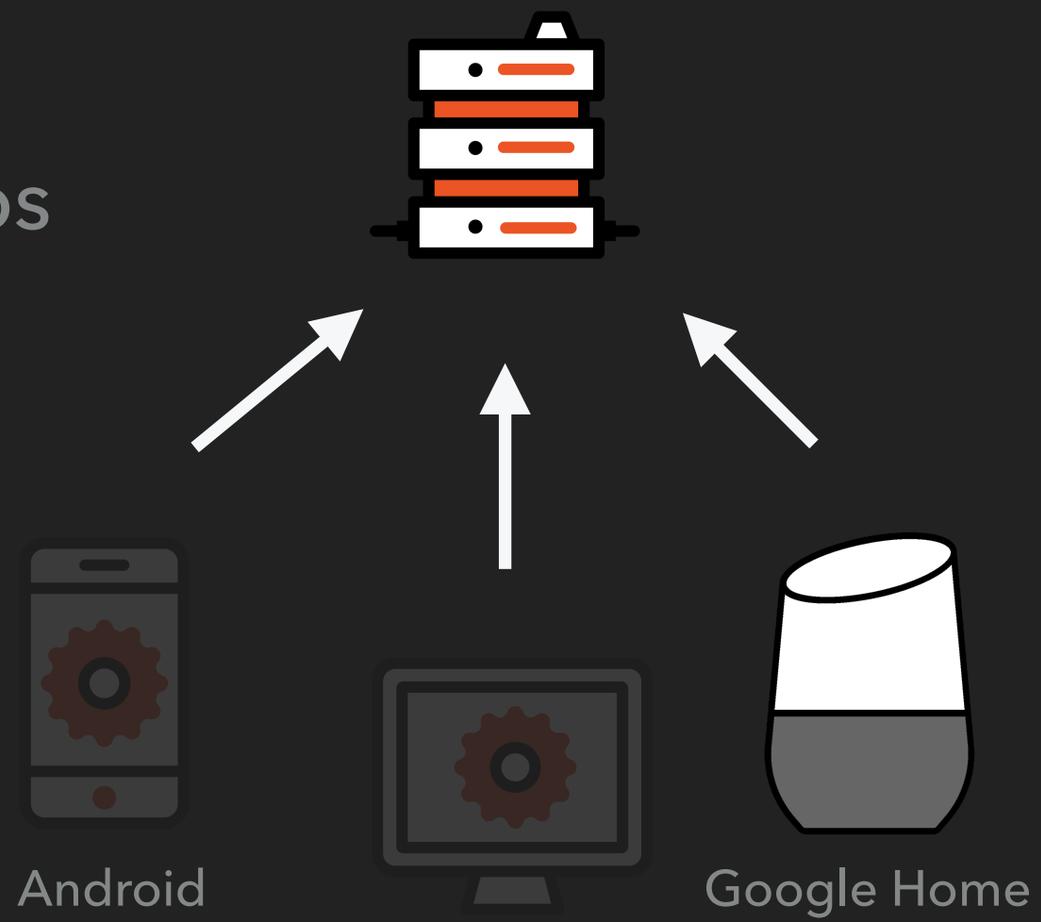


SIM, FUNCIONA. MAS...

@brunoskrebs

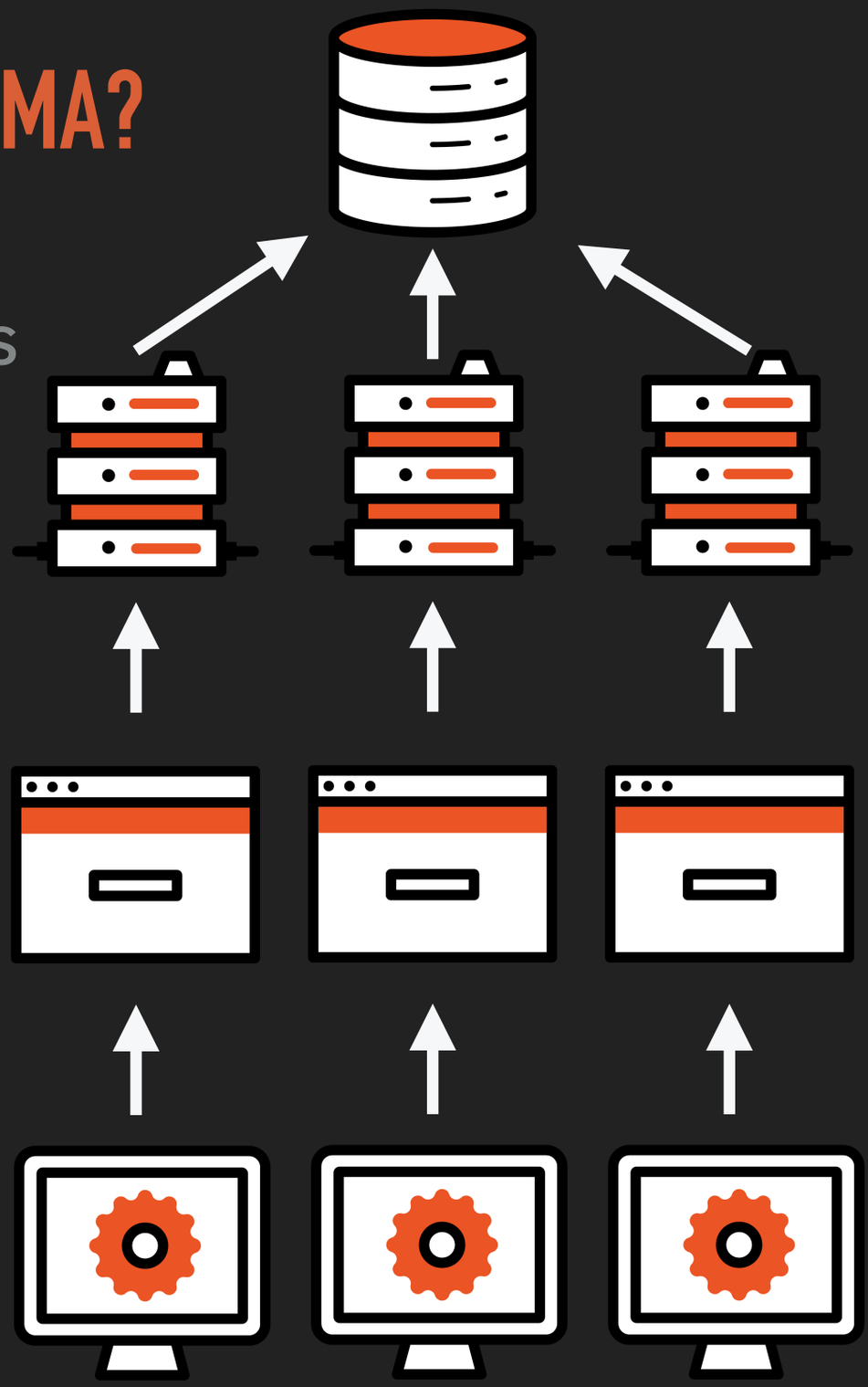
APLICAÇÕES TRADICIONAIS – PROBLEMA?

- Sim, quando diferentes aparelhos precisam se conectar



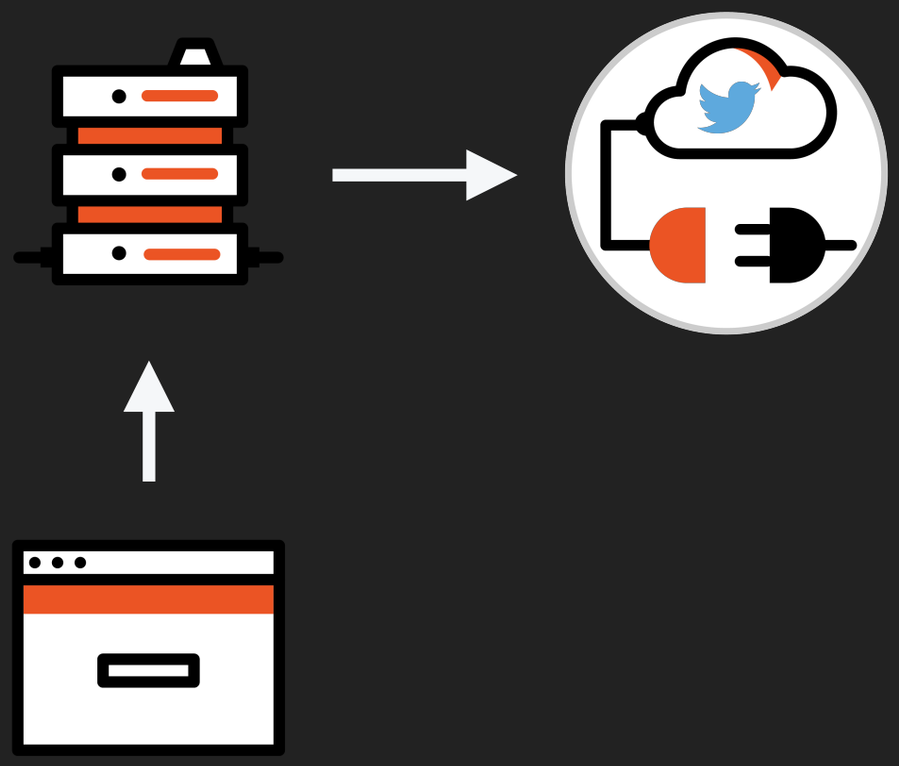
APLICAÇÕES TRADICIONAIS – PROBLEMA?

- Sim, quando diferentes aparelhos precisam se conectar
- Sim, fortemente acoplado



APLICAÇÕES TRADICIONAIS – PROBLEMA?

- Sim, quando diferentes aparelhos precisam se conectar
- Sim, fortemente acoplado
- Sim, se a aplicação precisar acessar algo em seu nome



APLICAÇÕES TRADICIONAIS – PROBLEMA?

- Sim, quando diferentes aparelhos precisam se conectar
- Sim, fortemente acoplado
- Sim, se a aplicação precisar acessar algo em seu nome
- Sim, dezenas de usuário e senha, ou reutilização de credenciais e senhas fracas

SOLUÇÃO?

OAUTH 2.0 E OPEN ID CONNECT

@brunoskrebs

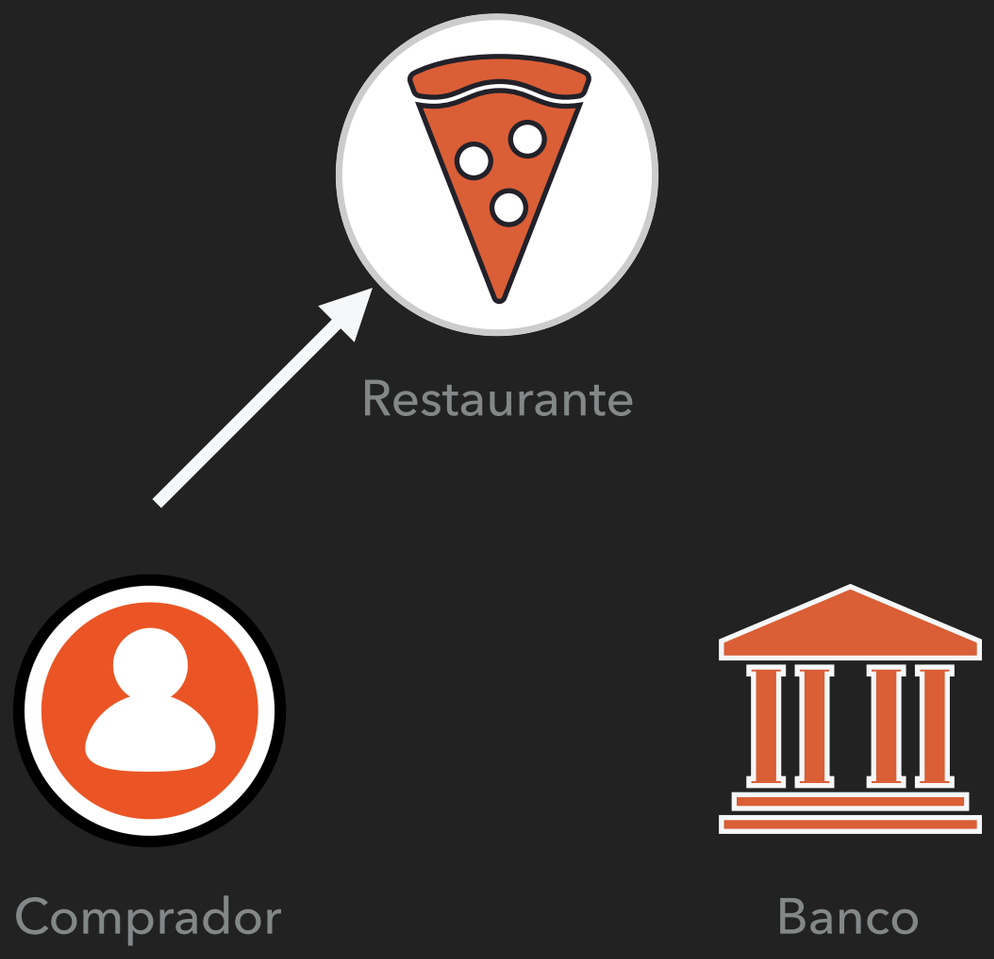
PROCESSO DE COMPRA

Restaurante

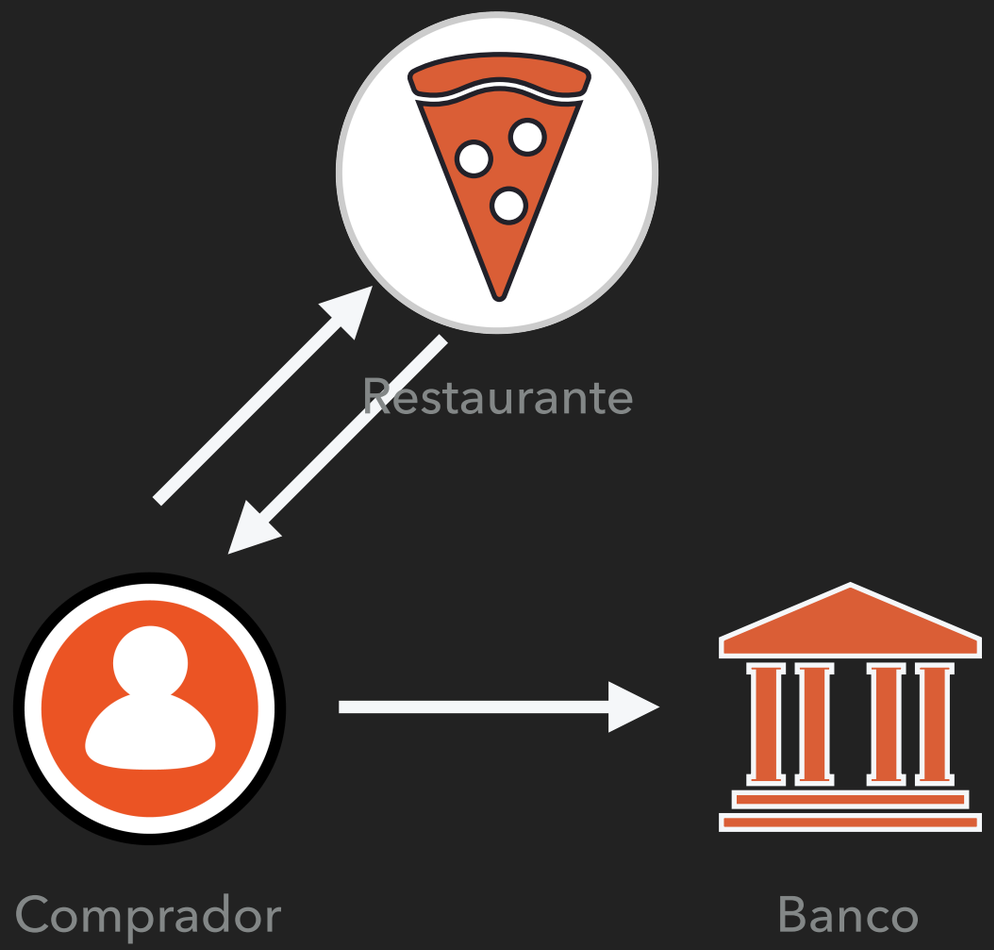
Comprador

Banco

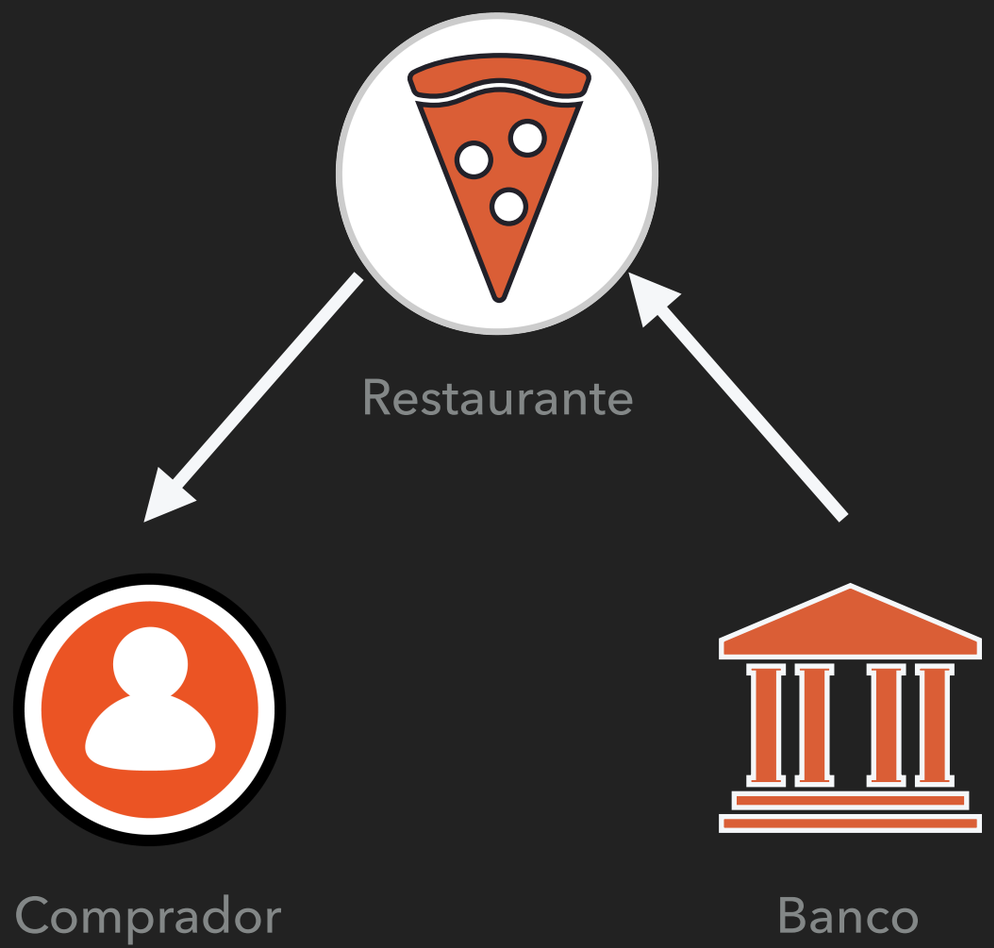
PROCESSO DE COMPRA



PROCESSO DE COMPRA



PROCESSO DE COMPRA



BASICAMENTE OAUTH 2.0!

@brunoskrebs

OAUTH 2.0 SIMPLIFICADO

Restaurante

Comprador

Banco

OAUTH 2.0 SIMPLIFICADO

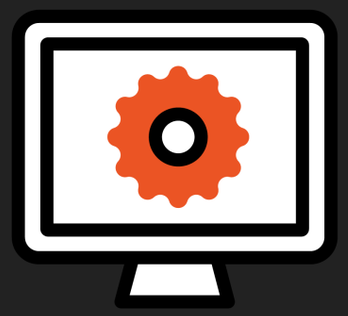
Restaurante

Aplicação

Banco

OAUTH 2.0 SIMPLIFICADO

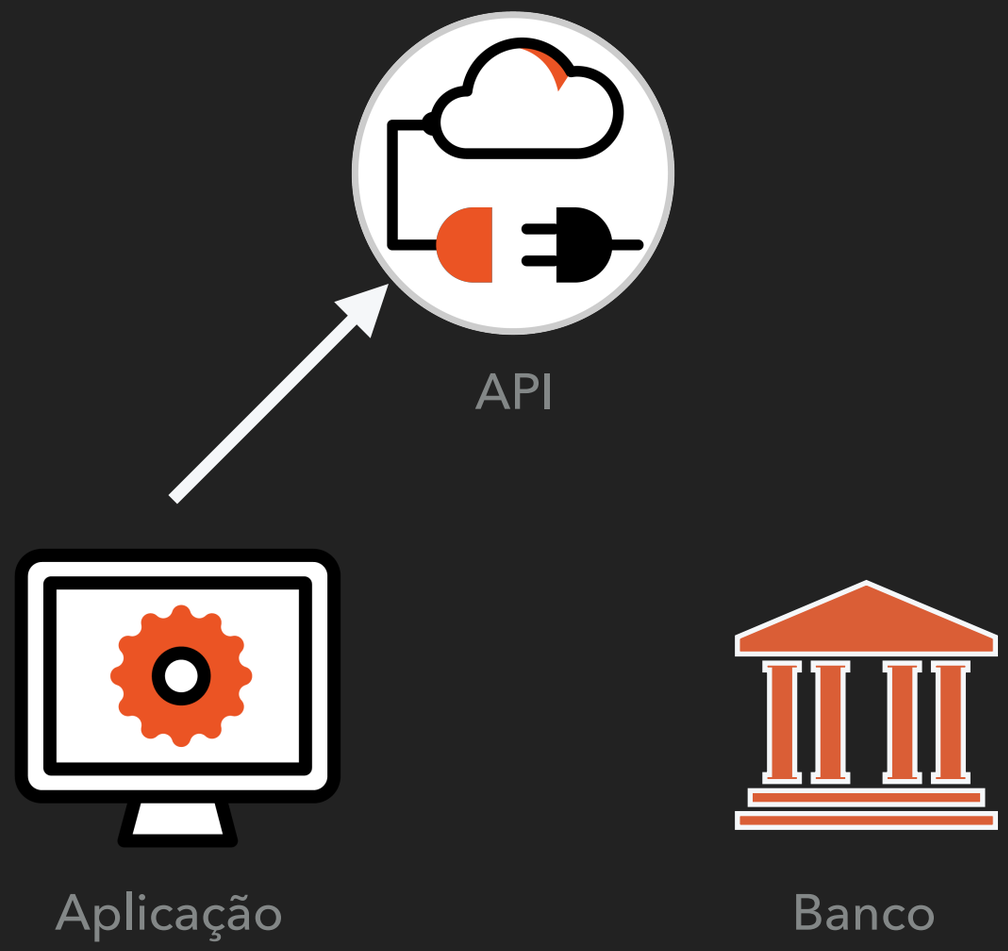
API



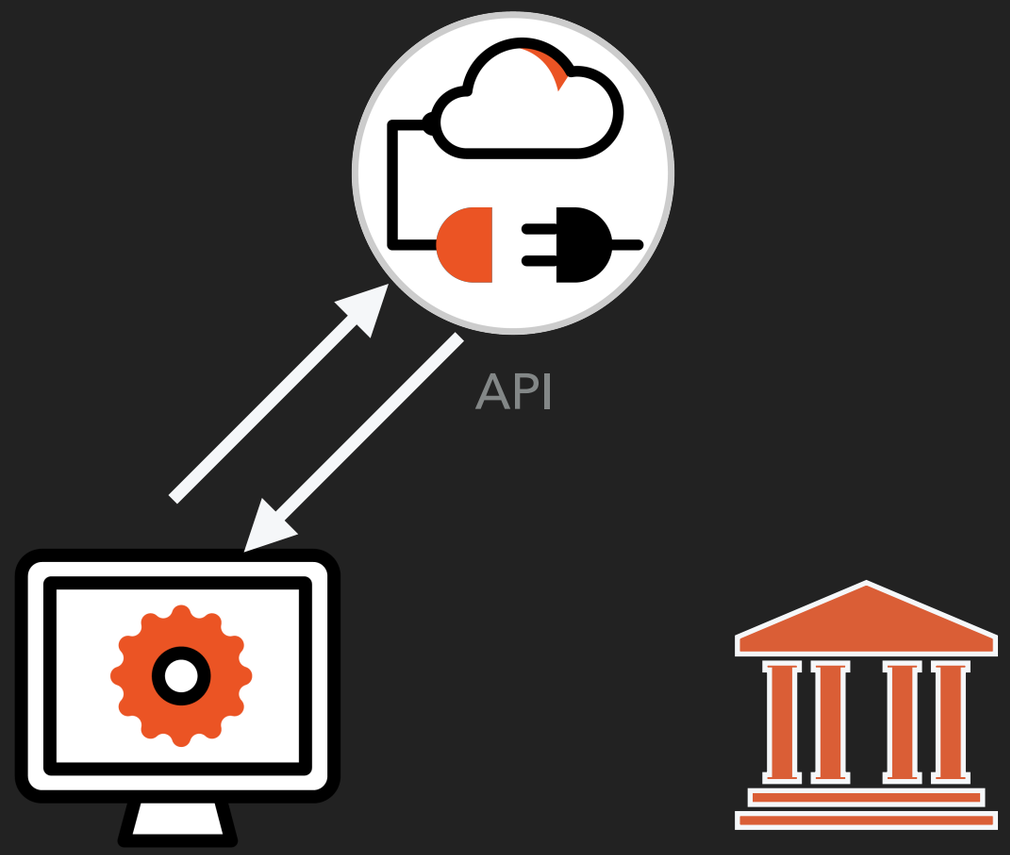
Aplicação

Banco

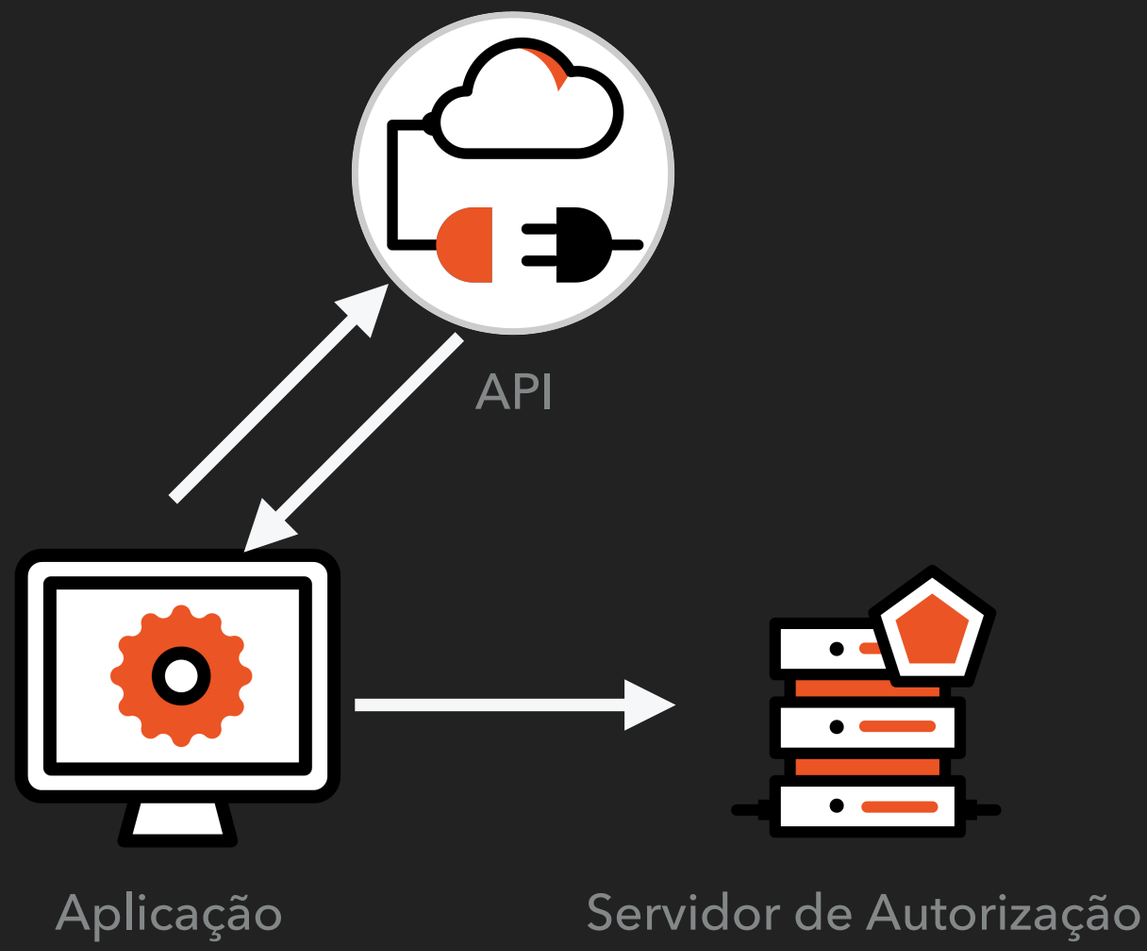
OAUTH 2.0 SIMPLIFICADO



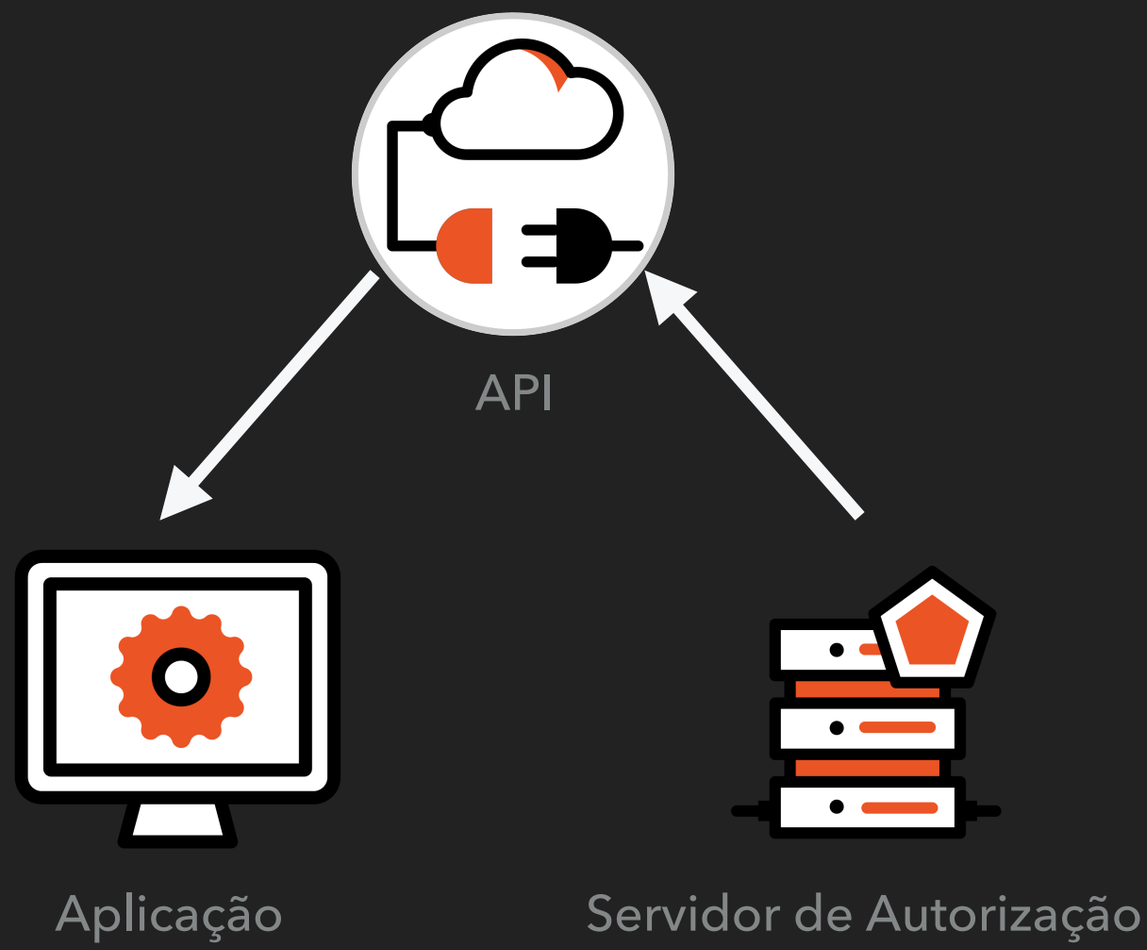
OAUTH 2.0 SIMPLIFICADO



OAUTH 2.0 SIMPLIFICADO



OAUTH 2.0 SIMPLIFICADO



OAUTH 2.0 SIMPLIFICADO

@brunoskrebs

OAUTH 2.0 – PARTES ENVOLVIDAS

API

OAUTH 2.0 – PARTES ENVOLVIDAS

Resource Server

OAUTH 2.0 – PARTES ENVOLVIDAS

Resource Server

Usuário

OAUTH 2.0 – PARTES ENVOLVIDAS

Resource Server

Resource Owner

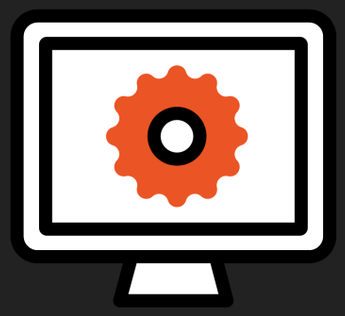
OAUTH 2.0 – PARTES ENVOLVIDAS

Aplicação

Resource Server

Resource Owner

OAUTH 2.0 – PARTES ENVOLVIDAS

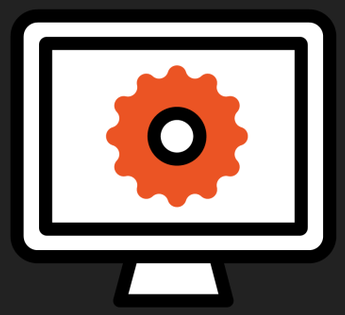


Client

Resource Server

Resource Owner

OAUTH 2.0 – PARTES ENVOLVIDAS



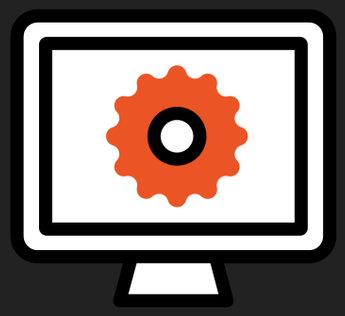
Client

Resource Server

Resource Owner

Servidor Autorização

OAUTH 2.0 – PARTES ENVOLVIDAS



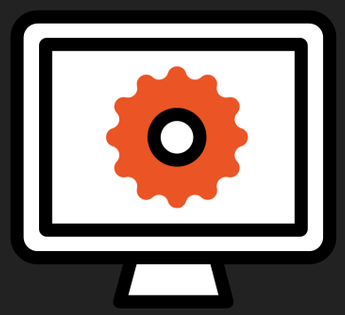
Client

Resource Server

Resource Owner

Authorization Server

OAUTH 2.0 – PARTES ENVOLVIDAS



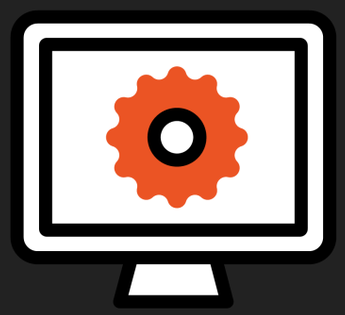
Client

Resource Server

Resource Owner

Authorization Server

OAUTH 2.0 – PARTES ENVOLVIDAS



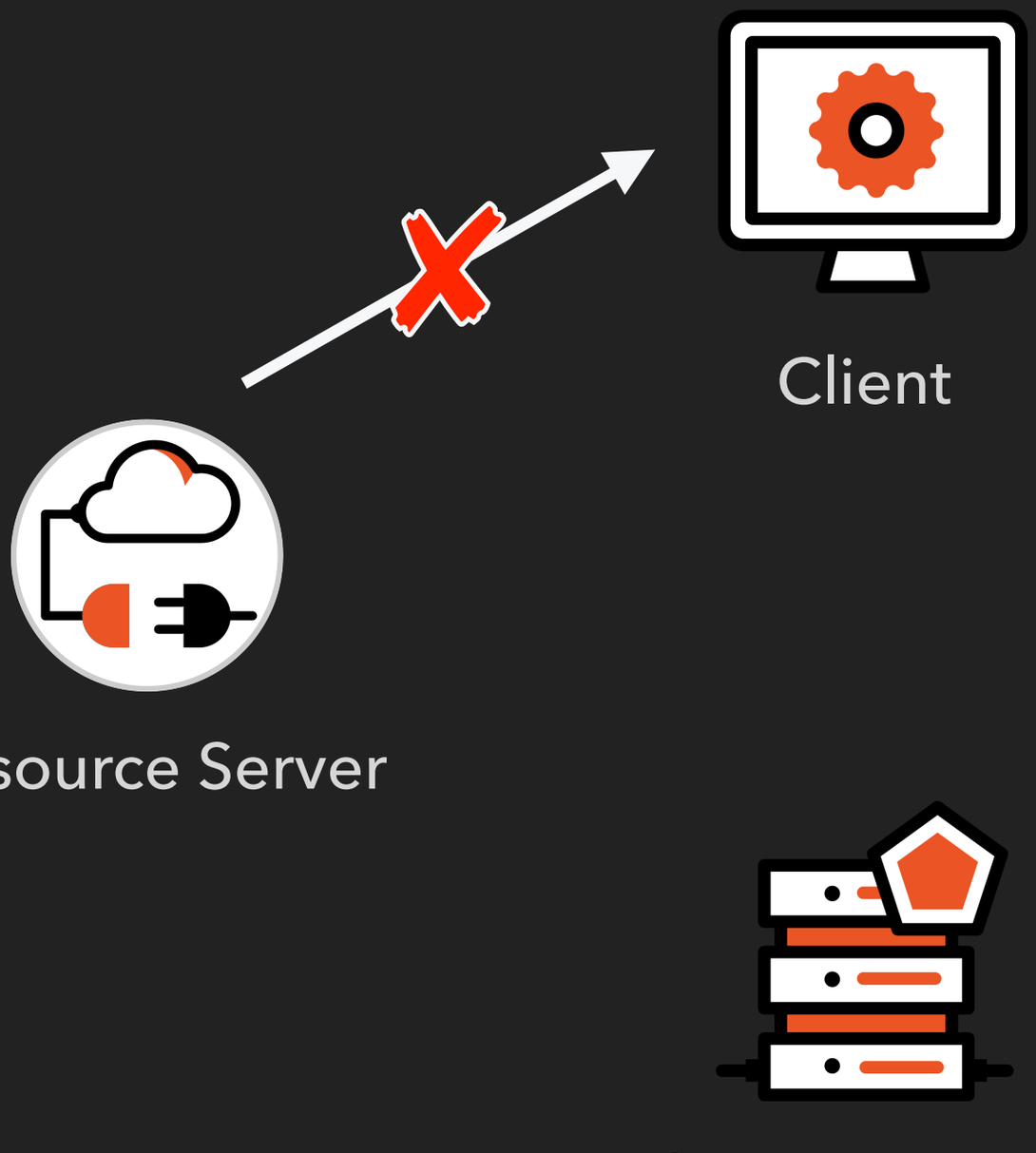
Client

Resource Server

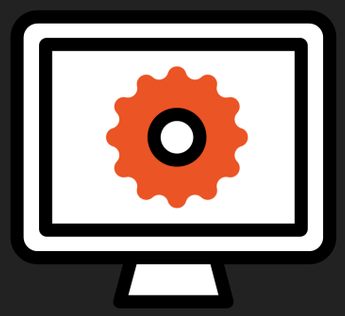
Resource Owner

Authorization Server

OAUTH 2.0 – PARTES ENVOLVIDAS



OAUTH 2.0 – PARTES ENVOLVIDAS



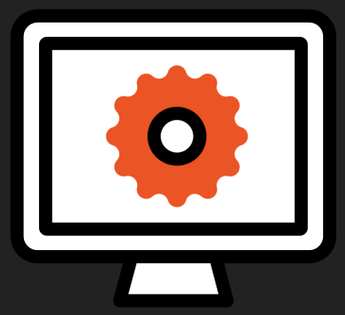
Client

Resource Server

Resource Owner

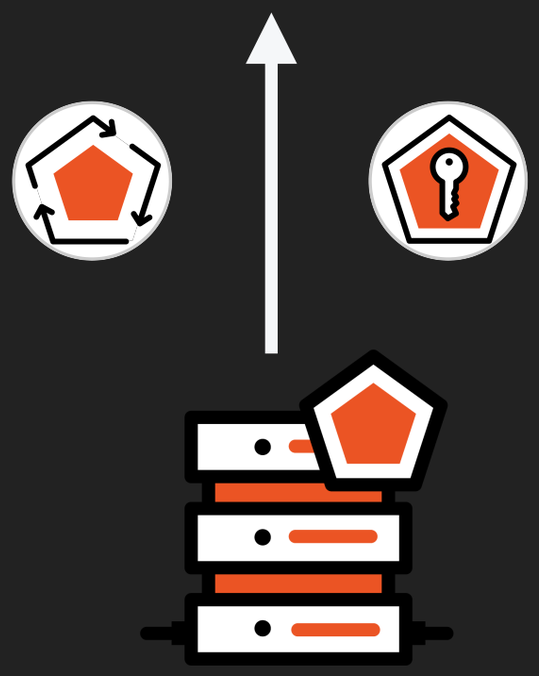
Authorization Server

OAUTH 2.0 – PARTES ENVOLVIDAS



Client

Resource Server



Authorization Server

Resource Owner

OAUTH 2.0 – TOKENS

- Access Tokens

- Dá acesso à um resource
- Serve como uma "procuração"
- Tempo de vida curto

- Refresh Tokens

- Permite que o AT seja renovado
- Tempo de vida longo
- Pode ser revogado

E O OPENID CONNECT?

@brunoskrebs

OPEN ID CONNECT

- Desenvolvido em cima do OAuth 2.0
- Não tem nada a ver com OpenID
- Prove informações sobre o usuário em um ID Token
- Define um endpoint no AS chamado /userinfo

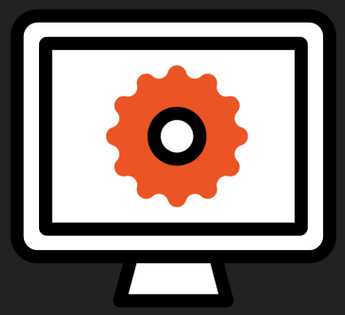
OPEN ID CONNECT

- Uses the "scope" to fetch info
  - openid
  - Profile
  - email
  - address
  - phone

OPENID CONNECT DEMO

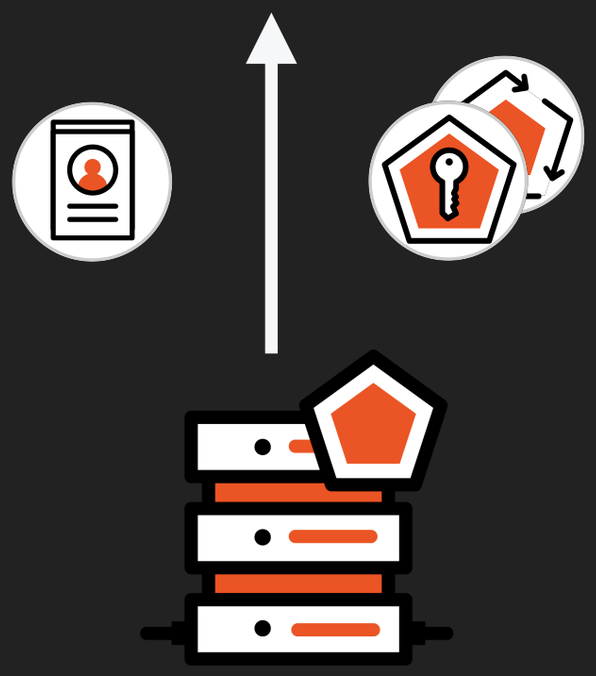
@brunoskrebs

OAUTH 2.0 – PARTES ENVOLVIDAS



Client

Resource Server



Authorization Server

Resource Owner

VANTAGENS

- Um usuário e senha a menos para lembrar
- Suporta diferentes tipo de aparelhos (móveis, SPAs, web apps, IoT, ...)
- Maior segurança (geralmente suportado por especialistas)
- Cloud Native
- Suporta Single Sing-On

SSO DEMO

@brunoskrebs

???

@brunoskrebs