Plataforma Node.js

Open Authorization (OAuth)

Prof. Rommel Vieira Carneiro

OAuth - Open Authorization

Descrição

- Framework aberto definido pelo IETF (RFC 6749)
- Foco na autenticação e autorização de recursos na Web

Características

- Evita exposição de senhas
- Facilita a interoperabilidade (Web, Mobile, Server)
- Controla a validade e o escopo do acesso concedido

OAuth – Papéis

Dono do Recurso

Servidor de Autorização

Papéis do OAuth

O mecanismo de autorização OAuth define quatro papéis.

Aplicação Cliente

Servidor de Recursos

OAuth – Papéis

Dono do Recurso

Dono do Recurso

Entidade que possui recursos na rede e pode ser solicitado a autorizar o acesso a estes recursos protegidos.

Ex: Usuário final

Servidor de Autorização

Aplicação Cliente

Servidor de Recursos

OAuth – Papéis

Dono do Recurso

Servidor de Autorização

Aplicação Cliente

Aplicação Cliente

Sistemas envolvidos que são utilizados para acessar recursos disponíveis na rede. Podem ser confidenciais ou públicos.

Ex: aplicações móveis e sites na Web

Servidor de Recursos

OAuth – Papéis

Dono do Recurso

Servidor de Autorização

Servidor de Autorização

Sistema que controla a geração de tokens de acesso para as aplicações cliente.

Ex: Google Accounts

Aplicação Cliente

Servidor de Recursos

OAuth – Papéis

Dono do Recurso

Servidor de Autorização

Servidor de Recursos

Ambiente que hospeda recursos protegidos na rede.

Ex: Google Fotos

Aplicação Cliente

Servidor de Recursos

OAuth – Access Token

- O Access Token é uma **credencial para acesso** a um recurso protegido.
- Trata-se de uma **string em formato específico** de acordo com a aplicação em questão
- Uma Access Token é obtida de acordo com o **tipo de autorização**
- A Access Token substitui a necessidade de **usuário e senha**

OAuth – Tipos de Autorização

O protocolo OAuth 2 oferece 4 tipos de autorização:

- Código de Autorização (*Authorization Code*)
- Autorização Implícita (*Implicit Grant*)
- Credenciais do Usuário (*Resource Owner Password Credentials*)
- Credenciais do Cliente (*Client Credentials*)

OAuth – Tipos de Autorização

O protocolo OAuth 2 oferece 4 tipos de autorização:

- Código de Autorização
  Ocorre quando a *Aplicação Cliente* é uma aplicação Web ou nativa e mantém uma chave secreta.
  Ex: Site X quer acessar seus dados no **facebook**
- Autorização Implícita
- Credenciais do Usuário
- Credenciais do Cliente

OAuth – Tipos de Autorização

O protocolo OAuth 2 oferece 4 tipos de autorização:

- Código de Autorização
- Autorização Implícita
  Ocorre quando a *Aplicação Cliente* é baseada no browser, em linguagem de script e não pode manter uma chave secreta.
  Ex: Aplicações SPA (Single Page Web)
- Credenciais do Usuário
- Credenciais do Cliente

OAuth – Tipos de Autorização

O protocolo OAuth 2 oferece 4 tipos de autorização:

- Código de Autorização
- Autorização Implícita
- Credenciais do Usuário
  Ocorre quando a *Aplicação Cliente* é próxima do *Servidor de Autorização* e requer usuário e senha, normalmente, ambos feitos pela mesma empresa.
  Ex: Aplicativo "Gerenciador de Negócios" do **facebook**
- Credenciais do Cliente

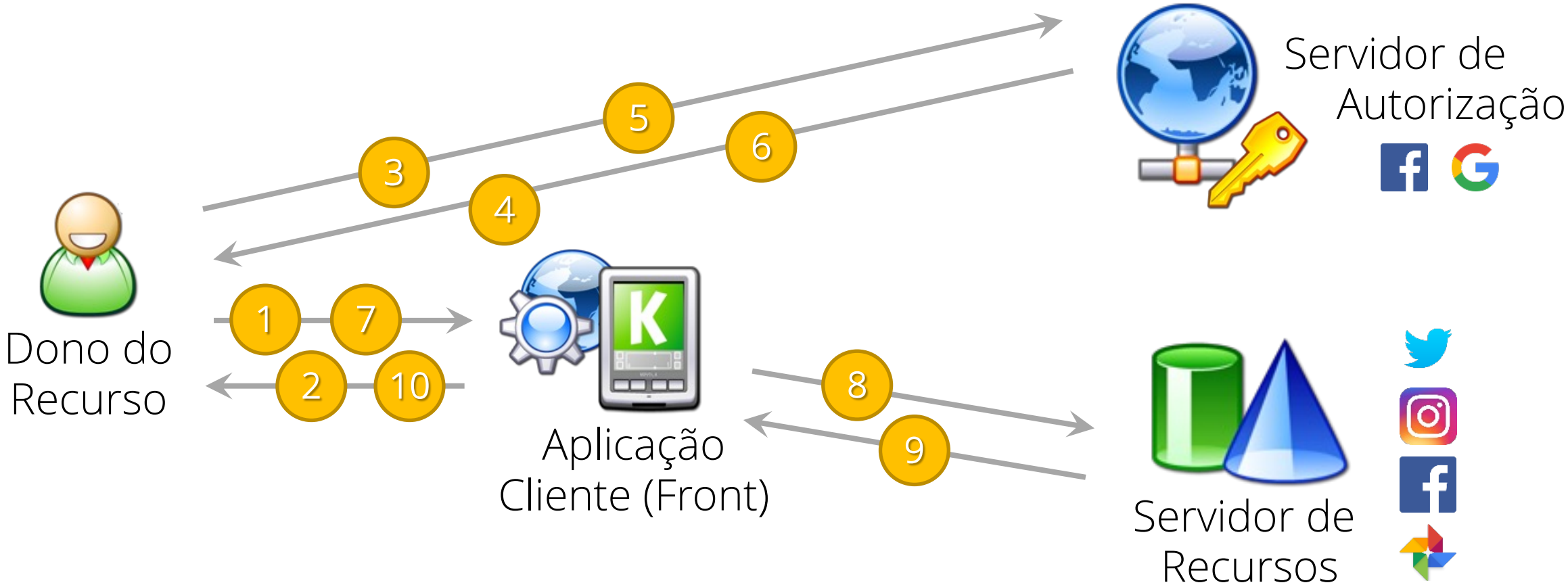
OAuth – Tipos de Autorização

O protocolo OAuth 2 oferece 4 tipos de autorização:

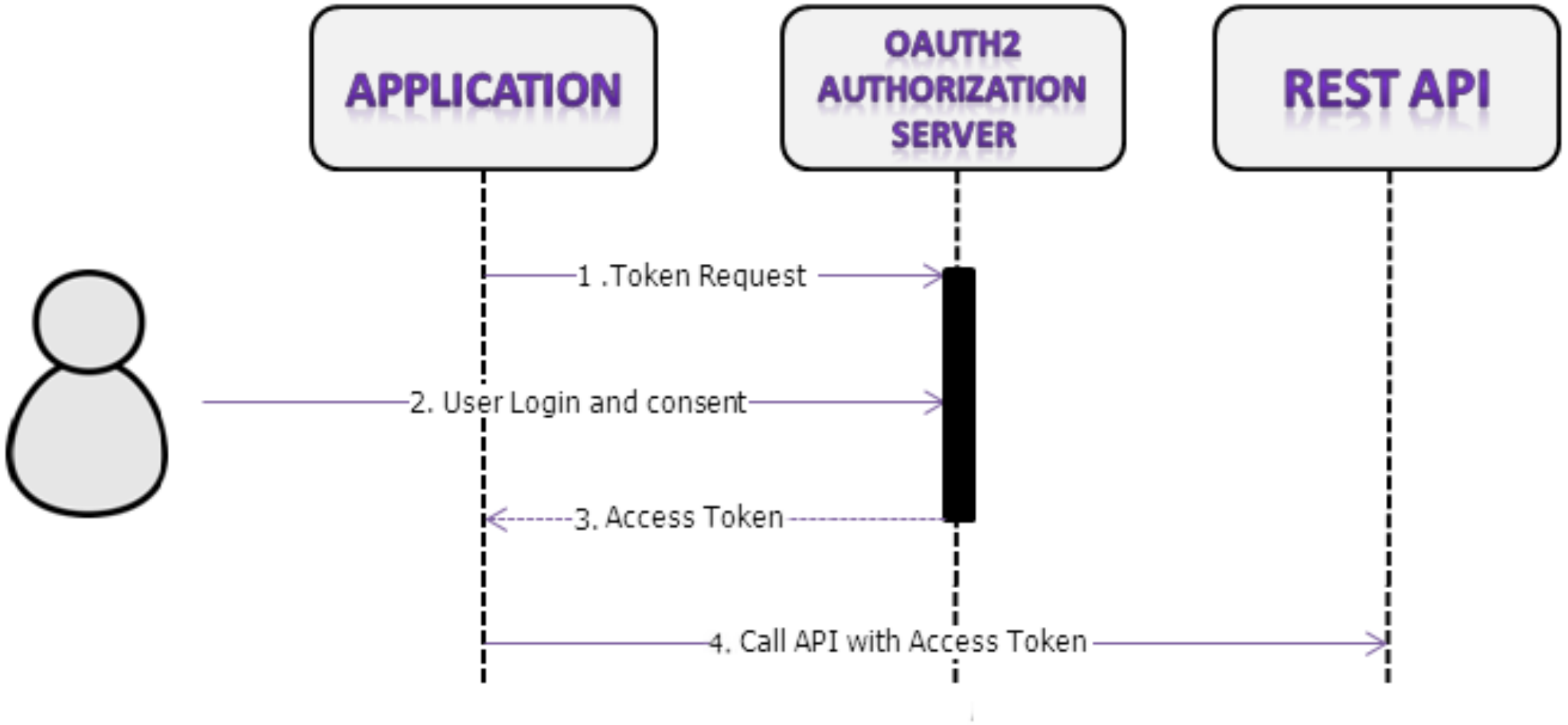
- Código de Autorização
- Autorização Implícita
- Credenciais do Usuário
- Credenciais do Cliente
  Ocorre quando a *Aplicação Cliente* é a proprietária dos recursos e não o usuário final.

  Ex: Cloud Azure acessando dados em storage interno

OAuth – Fluxos – Autorização Implícita

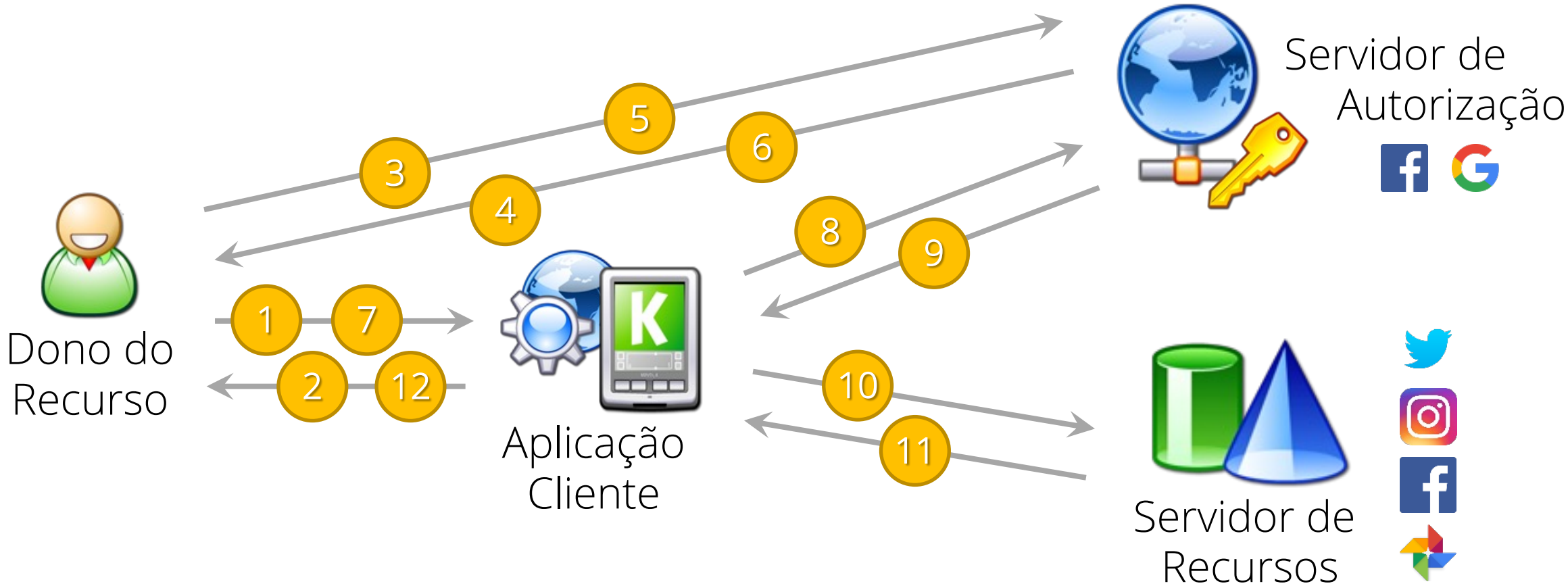


OAuth – Fluxos – Autorização Implícita

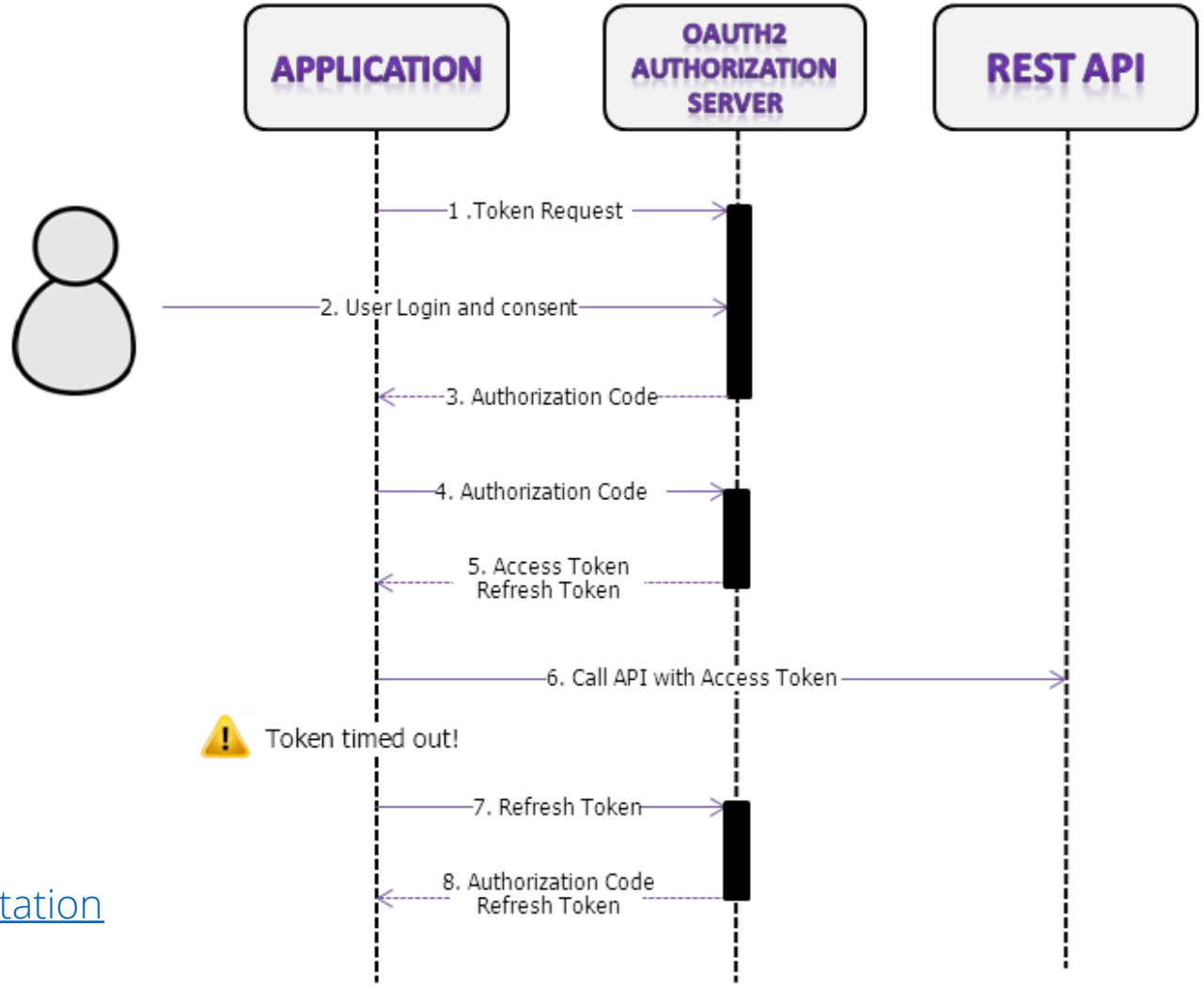


Fonte: [Qeo Native Documentation]

OAuth – Fluxos – Código de Autorização



OAuth – Fluxos – Código de Autorização



Fonte: [Qeo Native Documentation]

263

Obrigado!

Prof. Rommel Vieira Carneiro