

# Autenticação e Autorização

QXD0193 - Projeto de Interfaces Web

Prof. Bruno Góis Mateus ([brunomateus@ufc.br](mailto:brunomateus@ufc.br))

# Agenda

- Introdução
- Autenticação e Autorização
- JWT

# Introdução



# Introdução

- Nos dias atuais utilizamos cada vez mais softwares que possuem dados sensíveis:
  - Ex: Redes sociais, internet banking (pix), cliente de emails
- A segurança do dados utilizados por essas aplicações devem ser assegurados
- Dentre as estratégicas básicas existem temos:
  - Autenticação
  - Autorização

# Introdução

- Tais termos são bastante comuns no contexto de desenvolvimento de software
- É com o uso destas duas técnicas que garantimos uma maior segurança aos recursos protegidos de um sistema
- Por essa razão, vamos aprofundar um pouco nesse assunto e veremos como utilizar a autenticação e autorização de usuários na prática

# Autenticação vs Autorização



# Autenticação vs Autorização

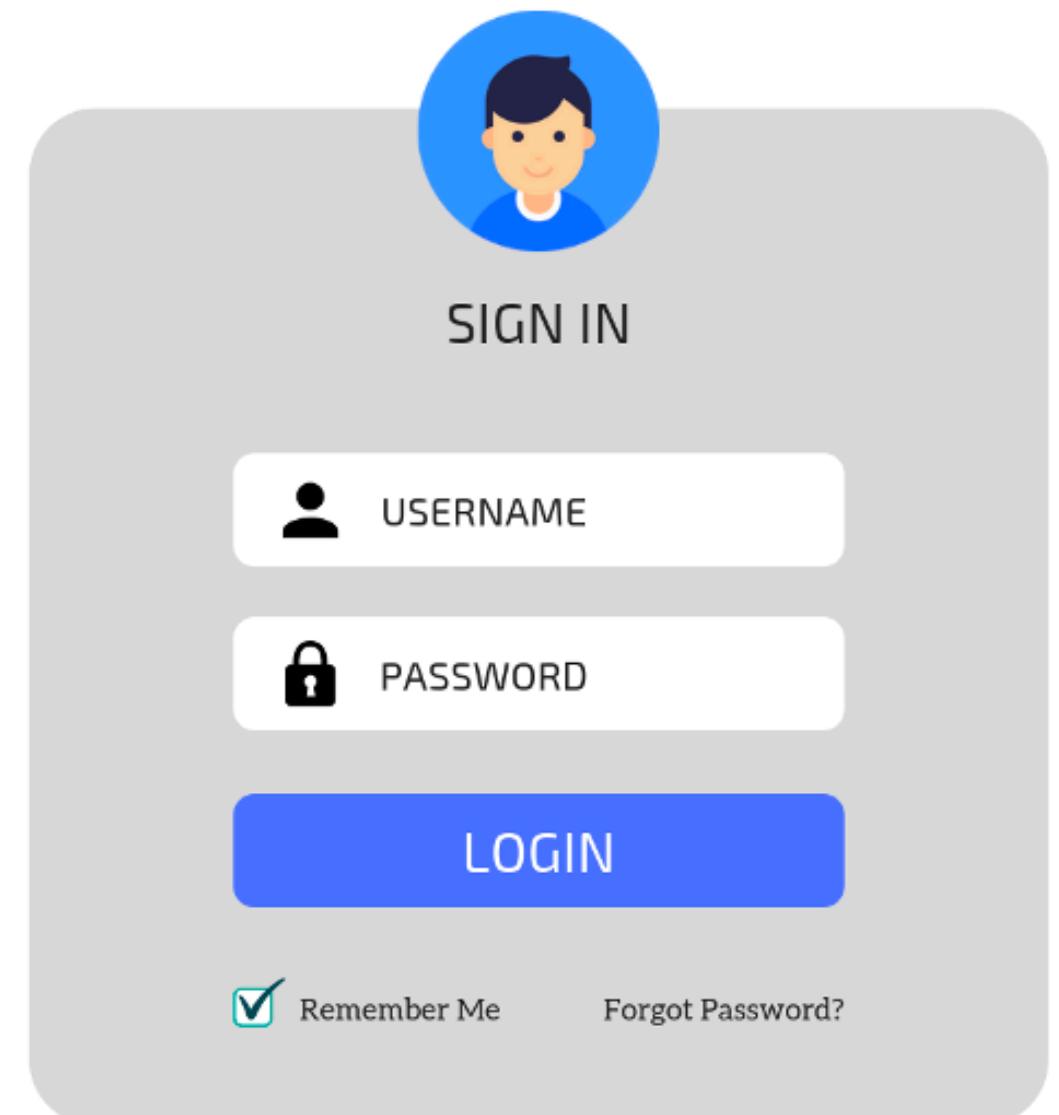
## Autenticação

- É o ato de provar a identidade de um usuário do sistema de computador
- Determina a identidade do usuário antes de revelar informações confidenciais
- Durante esse processo, o usuário faz uma afirmação comprovável sobre a identidade individual (sua) ou a identidade de uma entidade
- Ex: comparando a senha inserida com a senha armazenada no banco de dados

# Autenticação vs Autorização

## Métodos comuns de autenticação

- O que o usuário sabe
  - Mais comumente, uma senha, mas poderia ser uma resposta de uma pergunta secreta
- O que o possui
  - Um dispositivo ou aplicativo
  - Um token de segurança
  - Um cartão de identidade digital
- Quem o usuário é
  - Dados biométricos: digitais, scanner de retina, reconhecimento facial.



# Autenticação vs Autorização

## Quando ela ocorre?

- Quando o servidor ou aplicação precisa saber exatamente quem está tentando acessar as informações

# Autenticação vs Autorização

## Autorização

- É usada para determinar as permissões concedidas a um usuário autenticado
  - Ocorre após a autenticação
  - Determina o que o usuário pode ou não fazer
    - Permissões e privilégios

# Autenticação vs Autorização

## Métodos comuns de autorização

- *Role-based access control (RBAC)*
  - Da acesso ao usuário de acordo com o papel dele em uma organização

Papel	Poderes
Super Admin	Tem os acessos as funcionalidades administrativas e as funcionalidades dos outros papéis
Administrator	Tem acesso administrativo de apenas uma instância da aplicação
Editor	Pode publicar e editar postagens, incluindo postagens de outros usuários
Author	Pode escrever e publicar suas postagens
Contribuidor	Pode escrever postagens, mas não pode publicá-las
Assinante	Pode ler as postagens publicadas

# Autenticação vs Autorização

## Métodos comuns de autorização

- *Attribute-based access control (ABAC)*
  - Modelo de gerencia de permissão mais granular que o *RBAC*
  - Utiliza uma série específica de atributos
    - Papel na organização, localização, tempo de acesso, nome, IP

# Autenticação vs Autorização

## Quando ela ocorre?

- Quando um usuário determinar acessar uma parte ou funcionalidade do sistema cujo acesso é restrito a certos usuários

# Autenticação vs Autorização

## Autenticação

Determina se um usuário é realmente quem ele diz ser

Desafia o usuário a validar suas credenciais por meio de, ex: senhas, reconhecimento facial ...

Realizado antes da autorização

Geralmente, envia uma informação por meio de um token de identificação

Geralmente é governado pelo protocolo [OpenID Connect \(OIDC\)](#)

## Autorização

Determina se um usuário pode ou não acessar algo

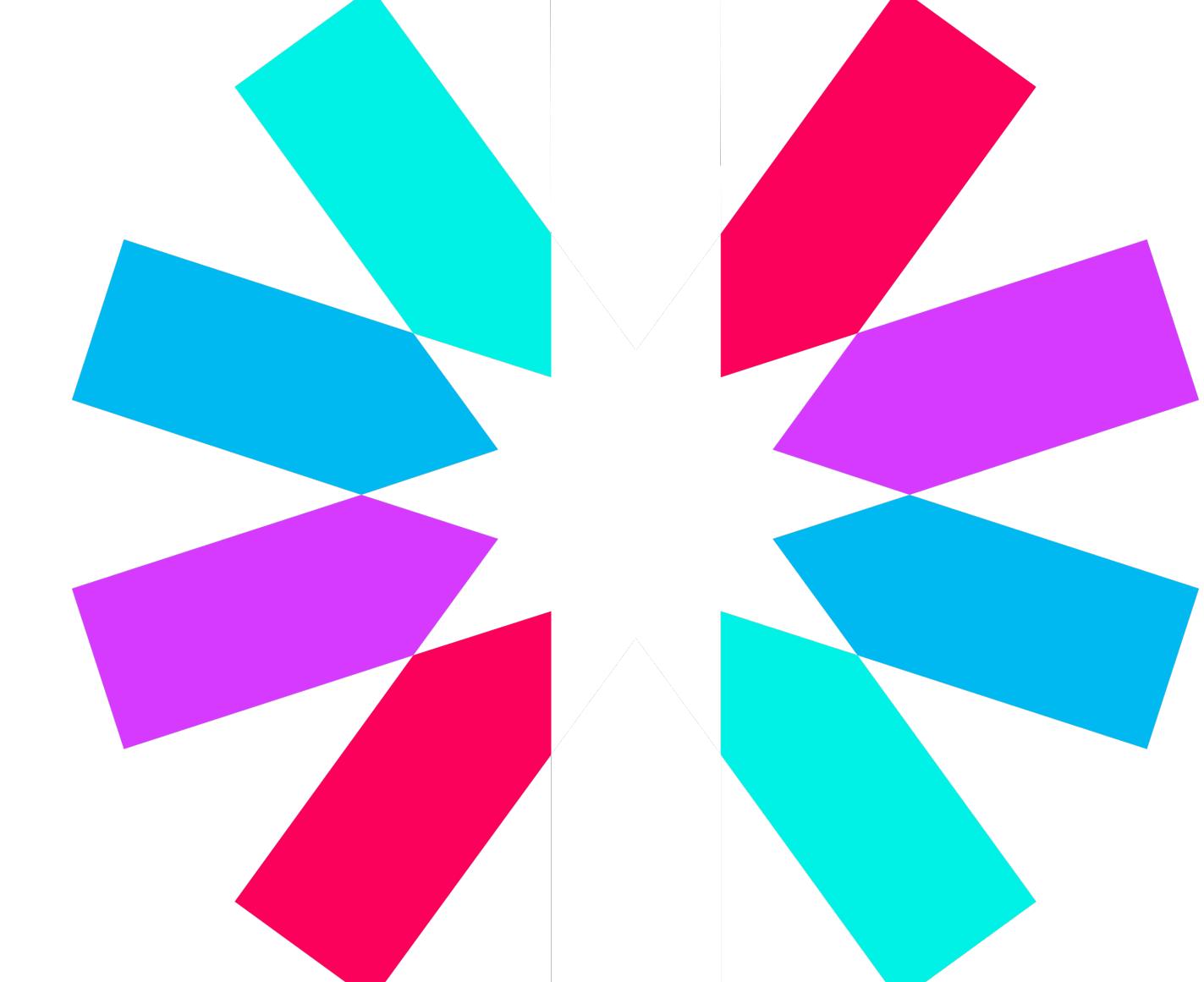
Verifica se um usuário tem acesso a algo baseado nas políticas e regras de acesso

Realizado após a autenticação

Geralmente, envia informações por meio de um token de acesso

Geralmente é realizado por meio do framework [OAuth 2.0](#)

JWT



# JWT

## Json Web Token

- Padrão aberto (RFC 7519) que define uma maneira de transmitir informações com segurança entre as partes como um objeto JSON
- Essas informações podem ser verificadas e confiáveis porque são assinadas digitalmente
- Podem ser assinados usando um segredo (com o algoritmo HMAC) ou um par de chaves pública/privada usando RSA ou ECDSA

# JWT

## Cenários de utilização

- Autorização
  - Cenário mais comum de sua utilização
  - Uma vez logado as requisições seguintes devem incluir o JWT
  - Permitindo o acesso a rotas, serviços e recursos garantido pelo token
  - Single Sign On (SSO) é um exemplo amplamente utilizado nos dias atuais que usa JWT devido a possibilidade de utilizado em diferentes domínios

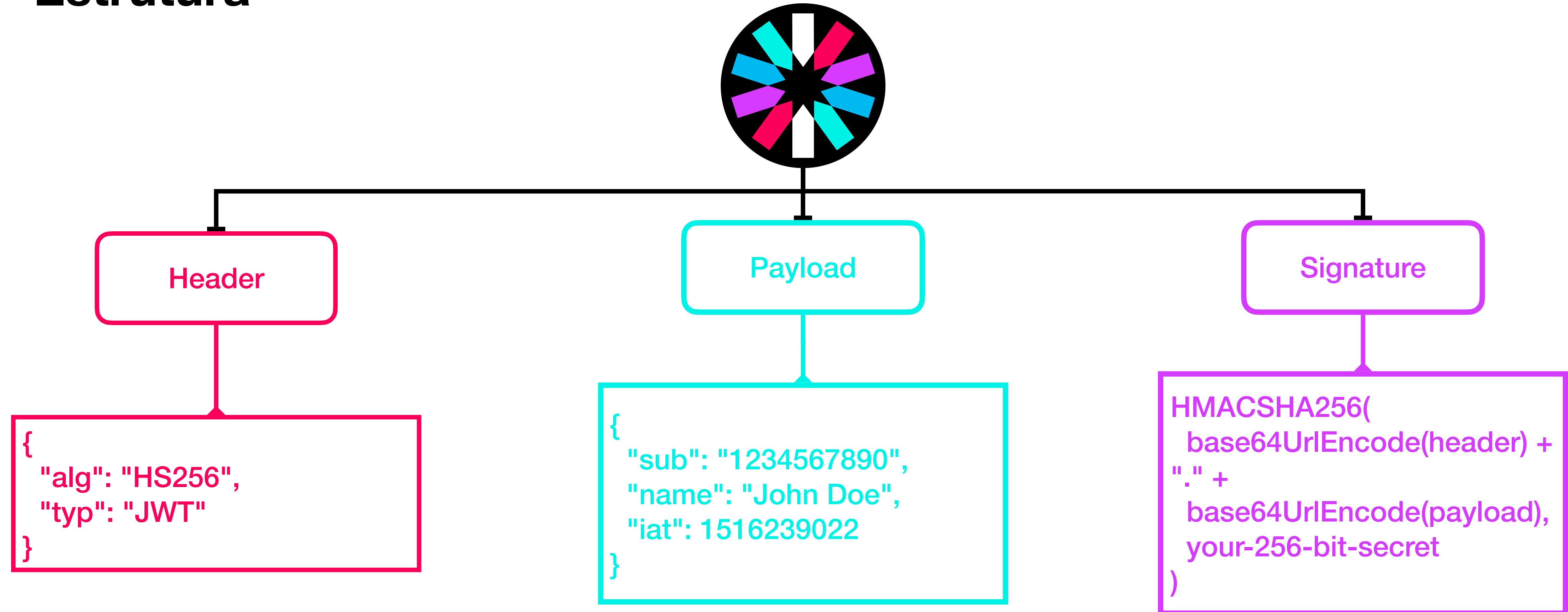
# JWT

## Cenários de utilização

- Troca de informações
  - JWT são uma maneira segura de trocar informações dado que eles podem ser assinados
    - Usando chaves públicas ou privadas
  - A assinatura é calculada a partir do *header* do *payload*, portanto é possível verificar se o token não foi adulterado

# JWT

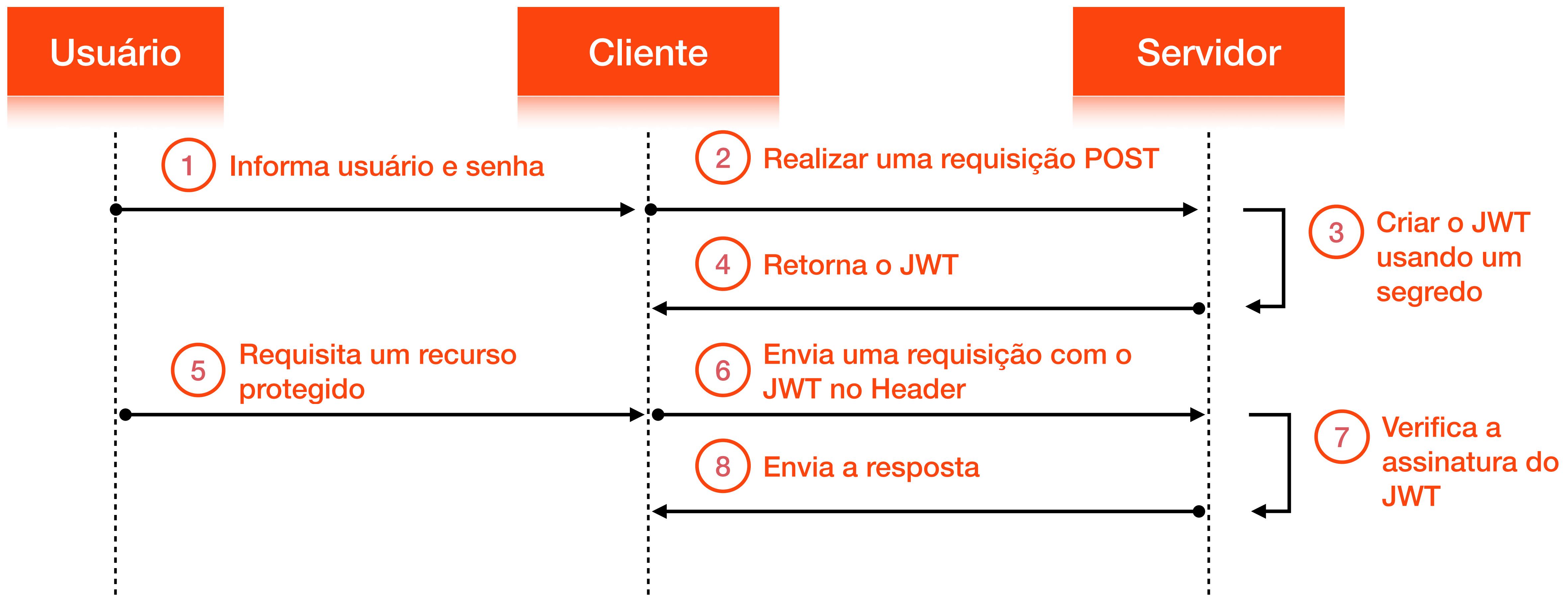
## Estrutura



eyJhbGciOiJIUzI1NilsInR5cCI6IkpXVCJ9 • eyJzdWliOilxMjM0NTY3ODkwIwibmFtZSI6IkpvaG4gRG9IliwiaWF0IjoxNTE2MjM5MDIyfQ • SflKxwRJSMeKKF2QT4fwpMeJf36POk6yJV\_adQssw5c

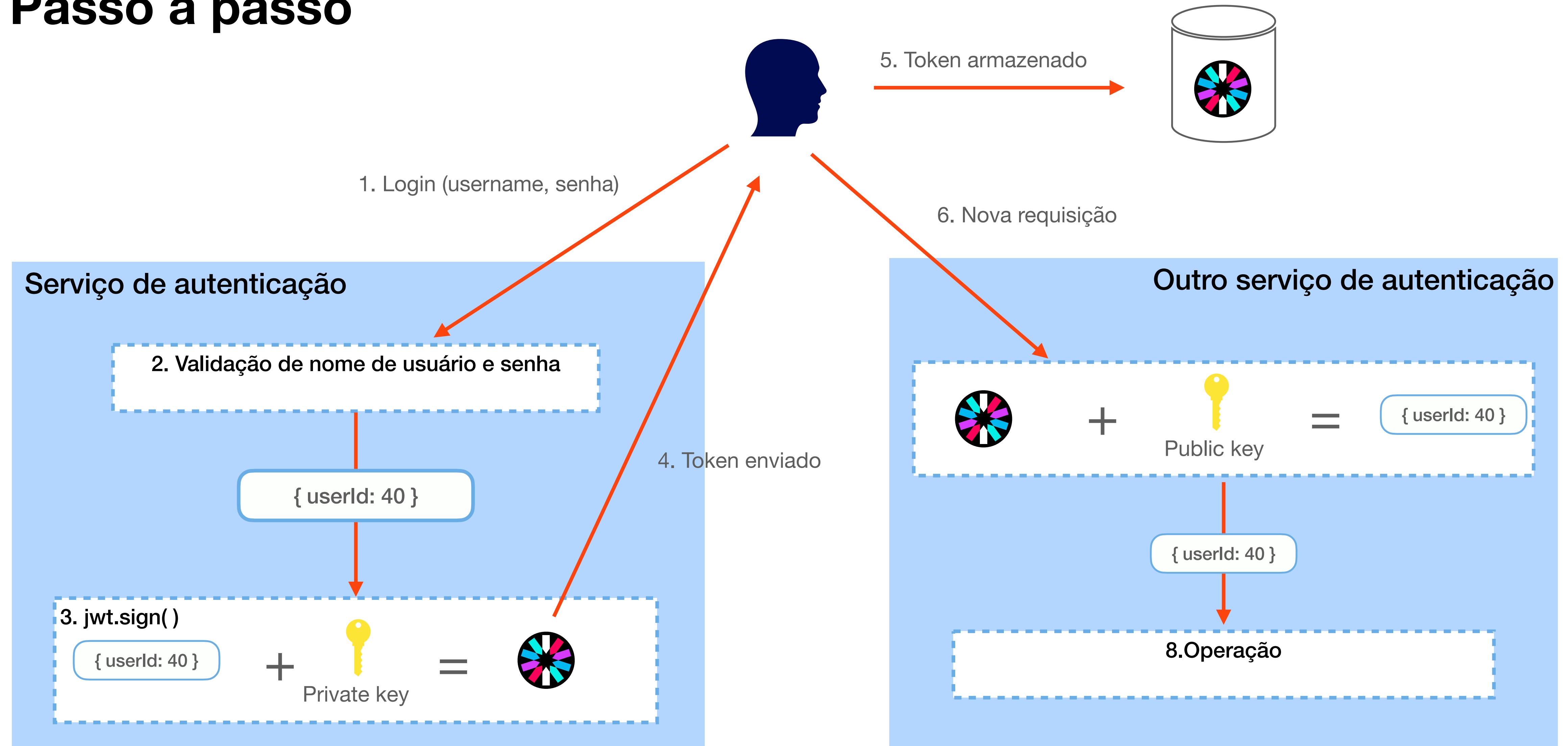
# JWT

## Passo a passo



# JWT

## Passo a passo



# Referências

- Autenticação, autorização e gerenciamento de identidade e acesso
- Autenticação x Autorização
- What Is the Difference Between Authentication and Authorization?
- Authentication vs. Authorization
- Understanding Authentication, Authorization, and Encryption
- Authentification in NodeJS with Express using JWT
- How to Build an Authentication API with JWT Token in Node.js

Por hoje é só