



API CARTEIRA E KEYCLOAK

Danubia Gama Macedo, Leonardo Queiroz e Wigor Ernandes
Prof. João Paulo Pretti - Engenharia de *Software*

Junho/2023
Cuiabá - MT

AGENDA

1. Introdução
2. Autorização e Autenticação
3. Conclusão
4. Considerações Finais

INTRODUÇÃO

KEYCLOAK

INTRODUÇÃO

O QUE É?

Keycloak é uma plataforma de código aberto para gerenciamento de identidade e acesso.

RECURSOS

Autenticação, autorização e gerenciamento de usuários, facilitando a implementação de segurança em aplicativos e serviços.

SUPORTES

- OAuth 2.0
- OpenID Connect

INTRODUÇÃO

FUNCIONALIDADES DO KEYCLOAK

- Autenticação por senha;
 - Autenticação social;
 - autenticação de dois fatores;
 - permissões granulares.
 - Gerenciamento de usuários;
 - Grupos e permissões;
 - Suporta integração com provedores externos;
-

INTRODUÇÃO

OAuth 2.0

O QUE É?

É um protocolo de autorização que permite que um usuário conceda acesso a determinados recursos a um aplicativo sem compartilhar suas credenciais de login.

COMO FUNCIONA?

- Redireciona para serviço de autenticação de terceiros (rede social por exemplo)
- Gera um token de acesso
- O token possui informações protegidas do usuário, sem acesso a informações de login.

INTRODUÇÃO

OpenID Connect

O que é?

É uma camada de autenticação baseada no OAuth 2.0. Ele adiciona uma camada de identidade à estrutura do OAuth 2.0, permitindo que aplicativos obtenham informações adicionais sobre o usuário autenticado.

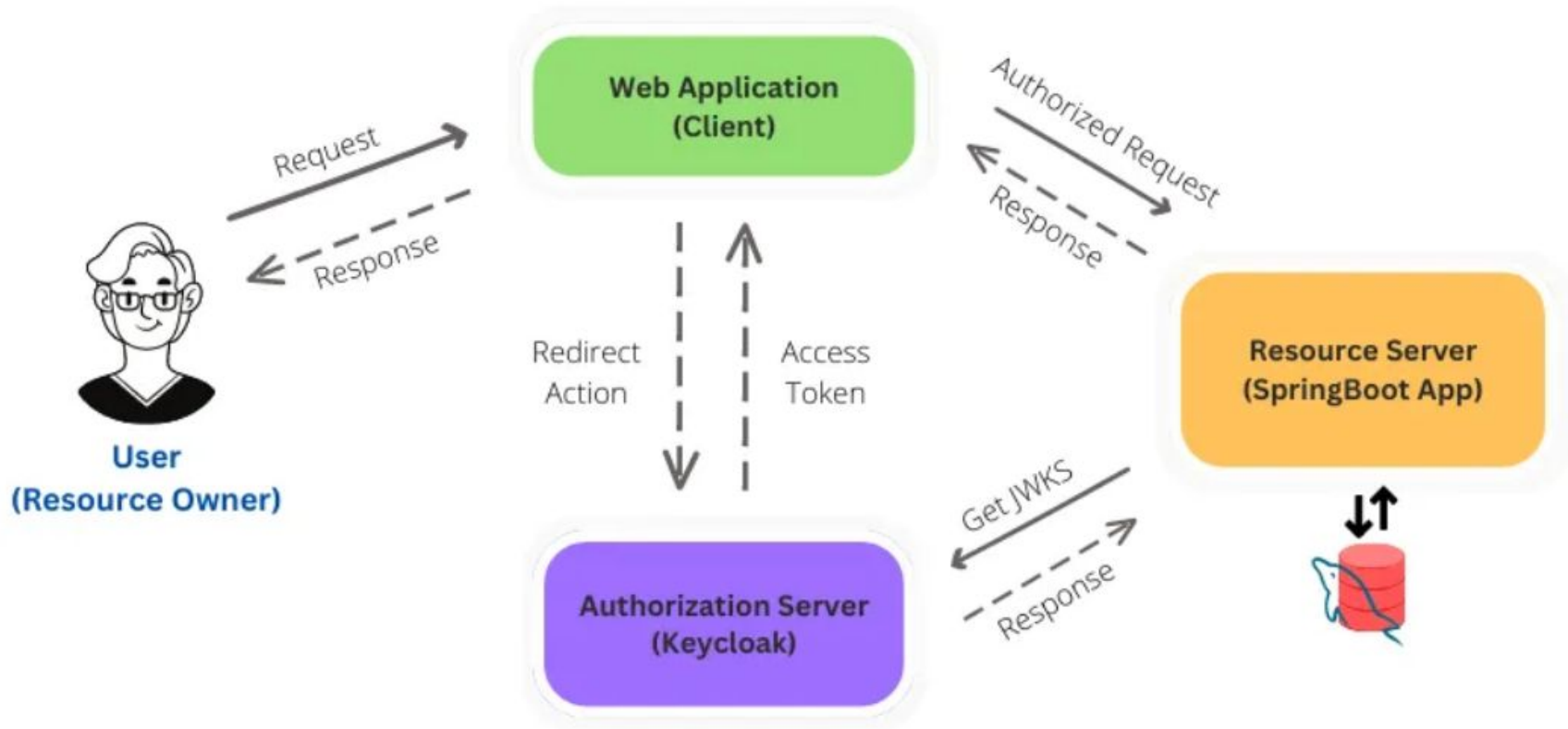
O que ele fornece?

- ID Token, que é um token criptográfico contendo informações sobre o usuário, como nome, endereço de e-mail, foto de perfil, entre outros.
- Um meio seguro para o aplicativo confirmar a autenticidade do usuário.

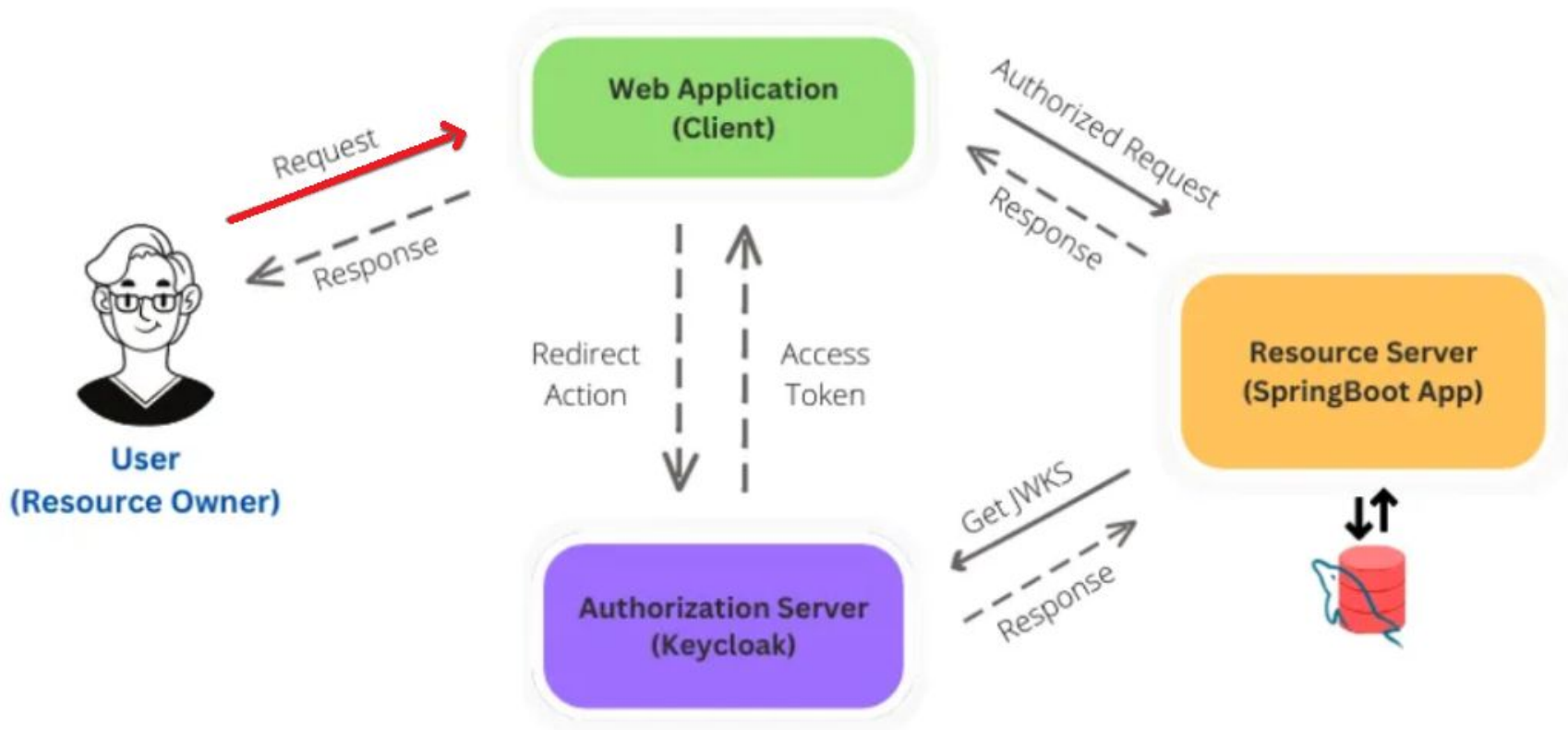
AUTENTICAÇÃO E AUTORIZAÇÃO

KEYCLOAK
E
SPRING SECURITY

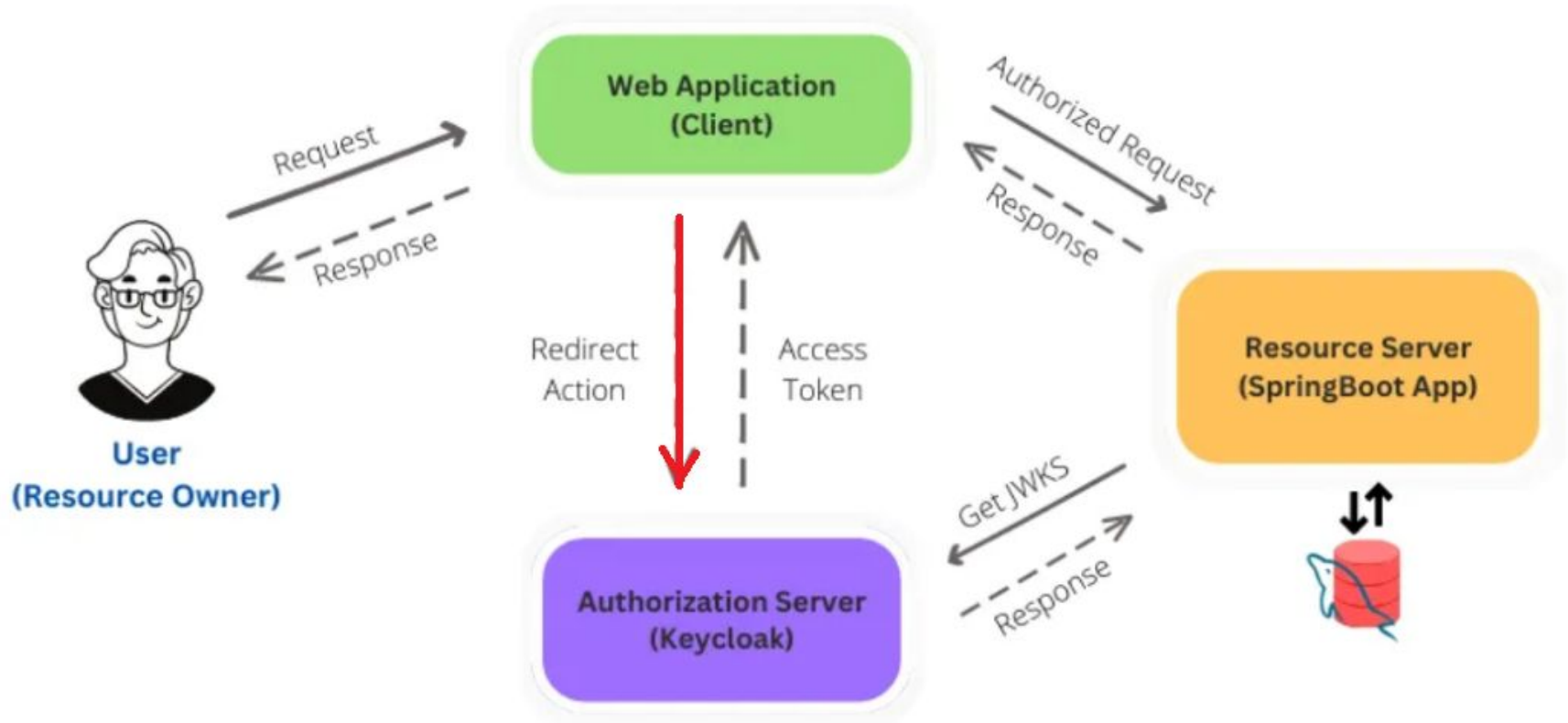
FLUXO



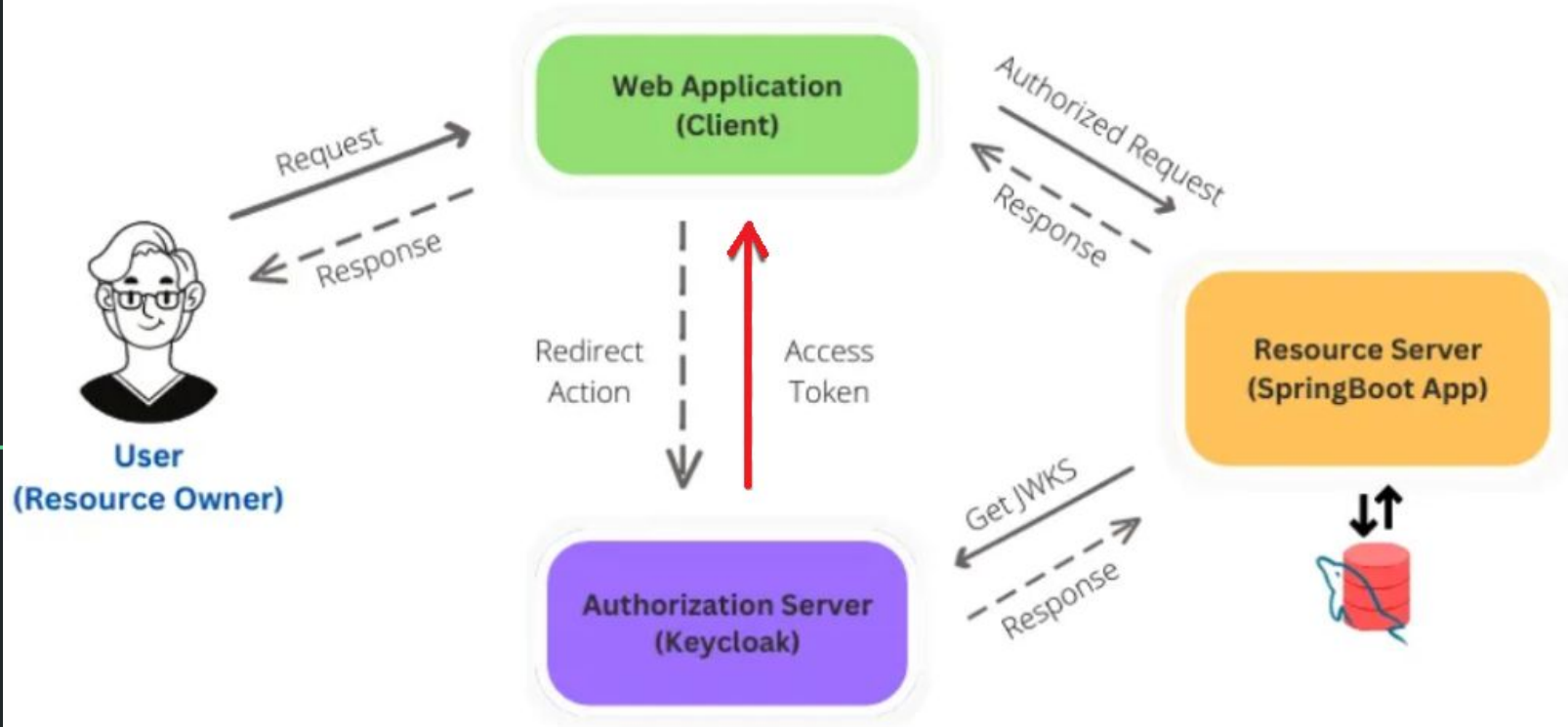
FLUXO



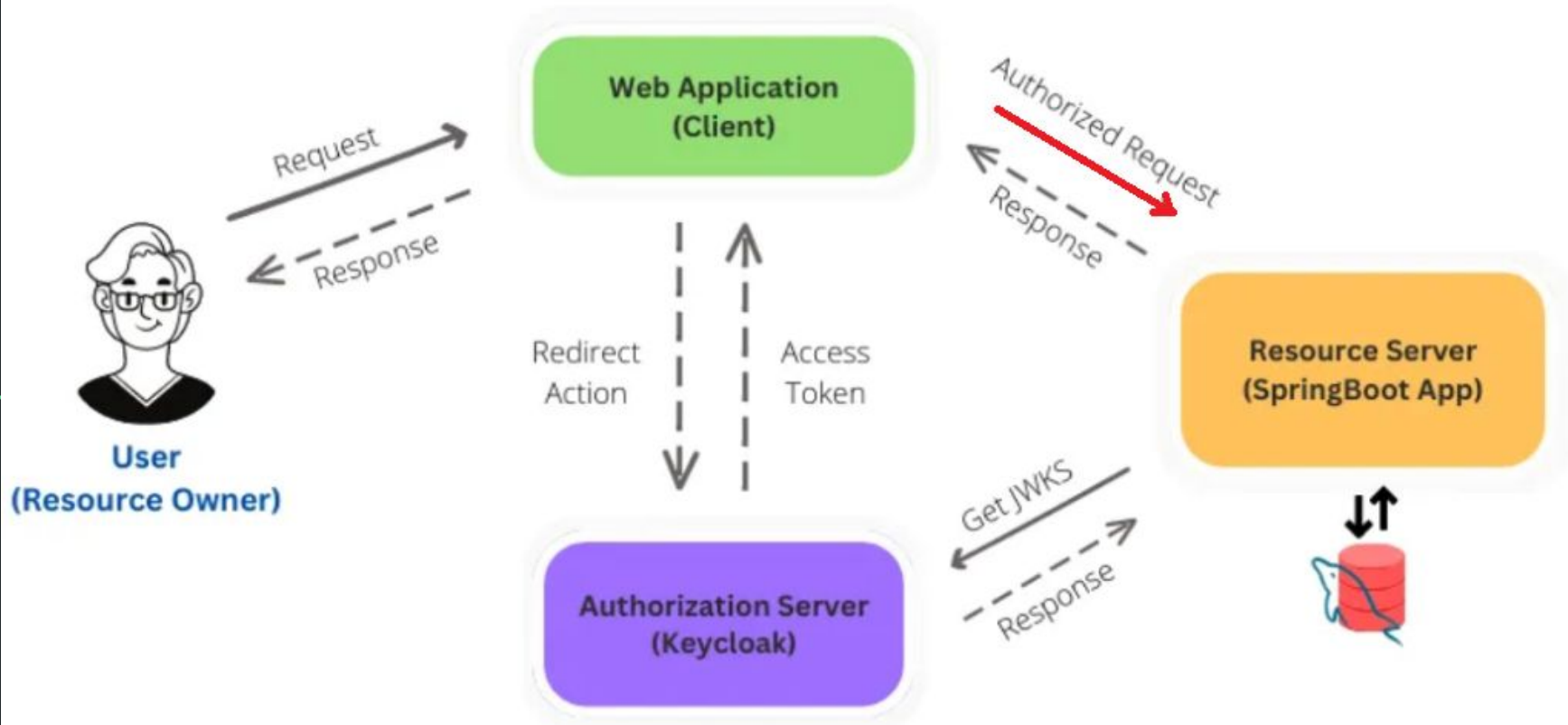
FLUXO



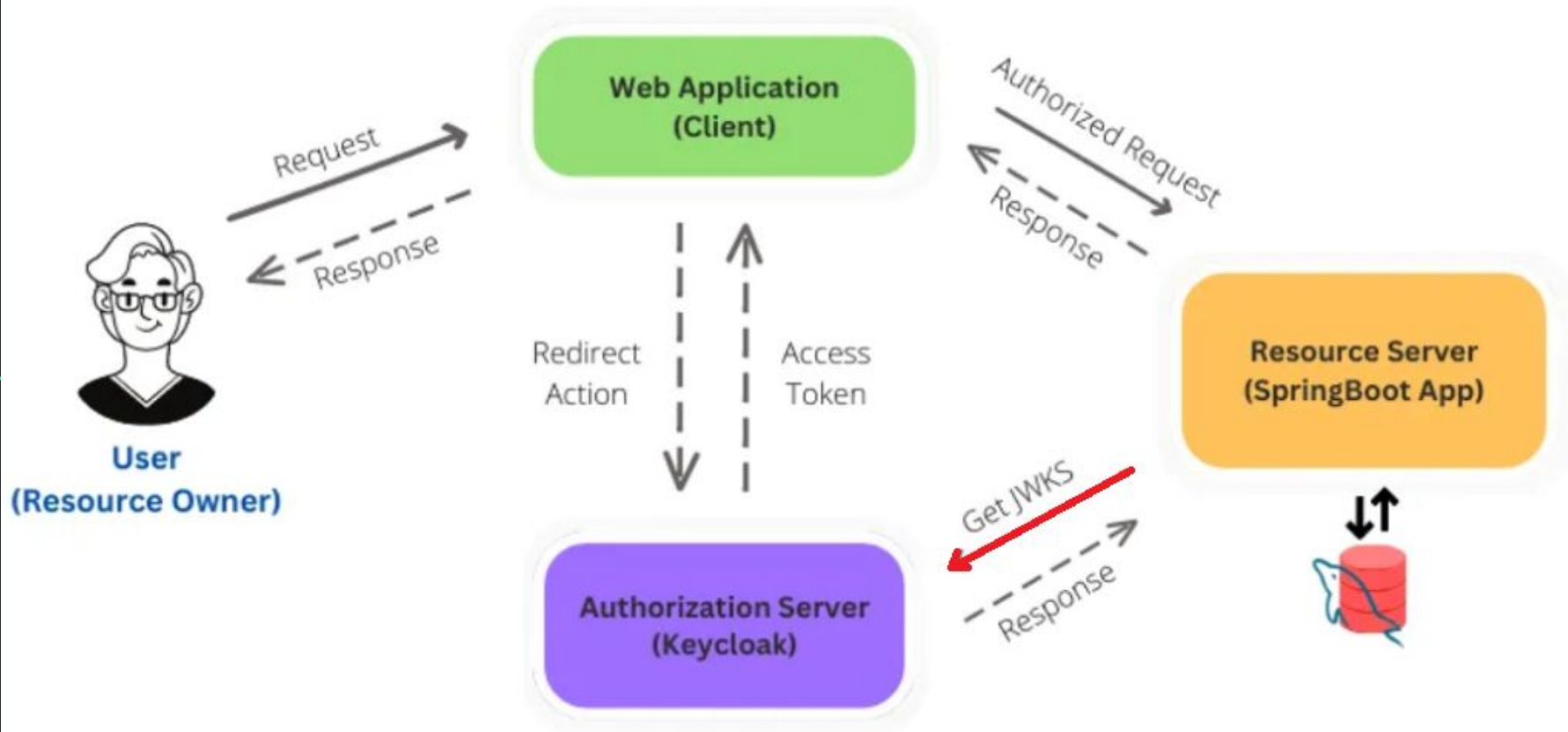
FLUXO



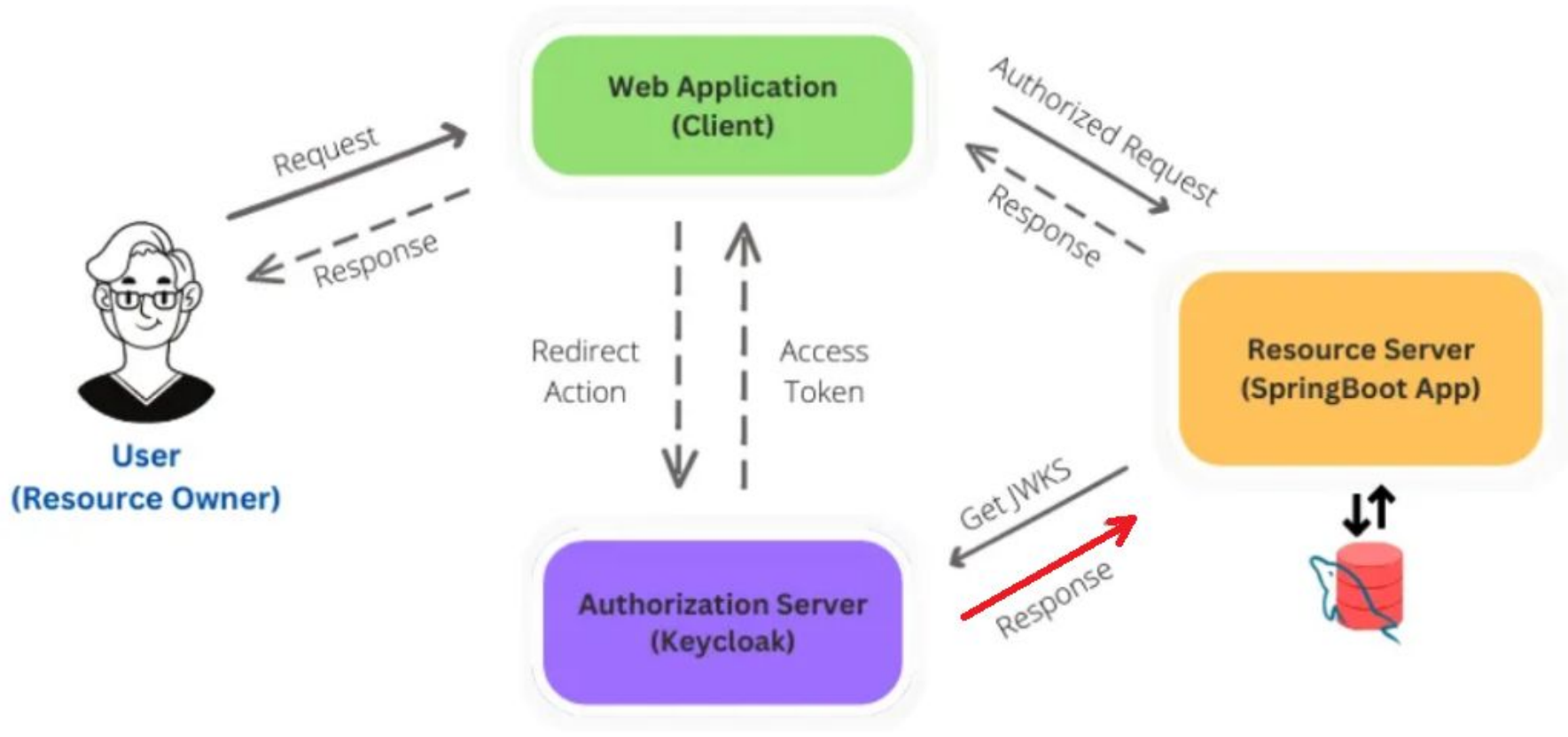
FLUXO



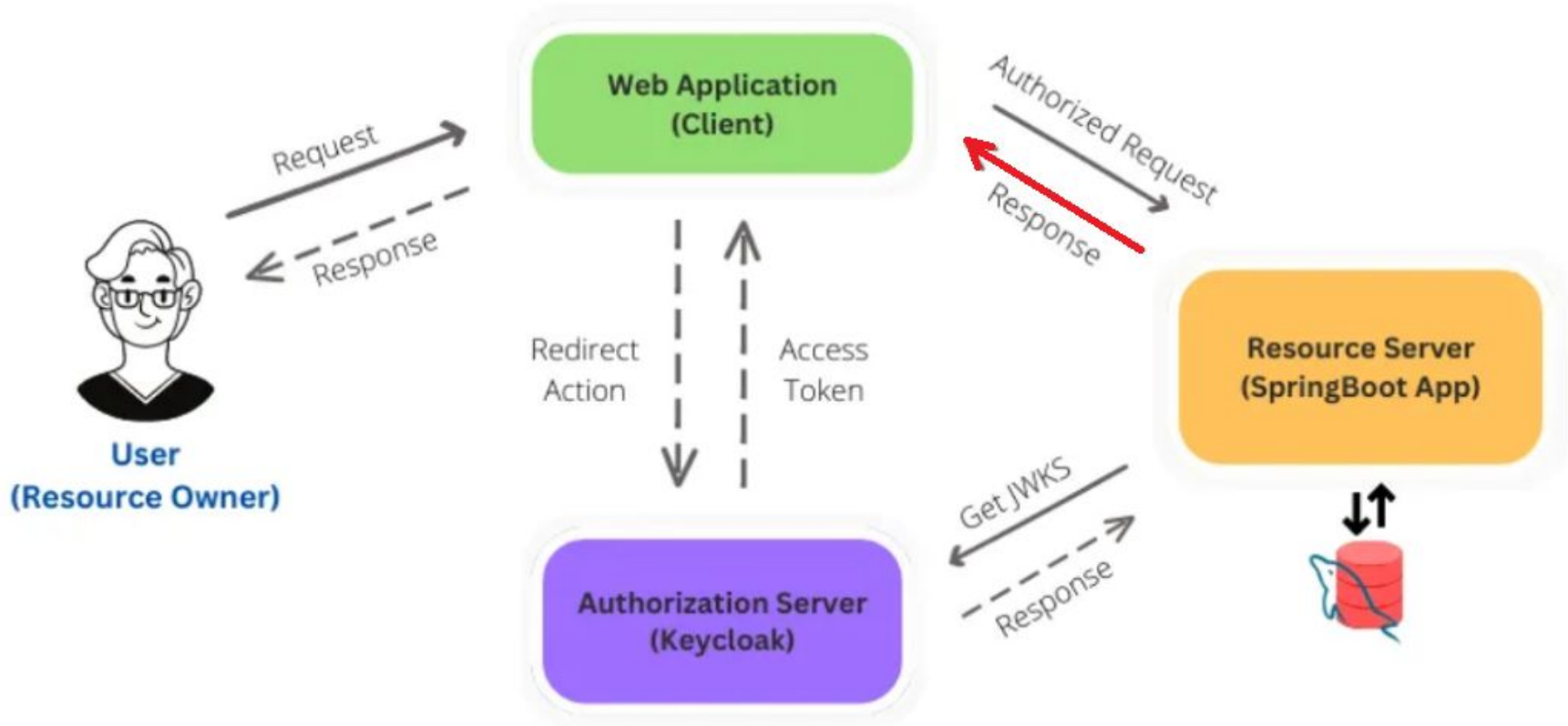
FLUXO



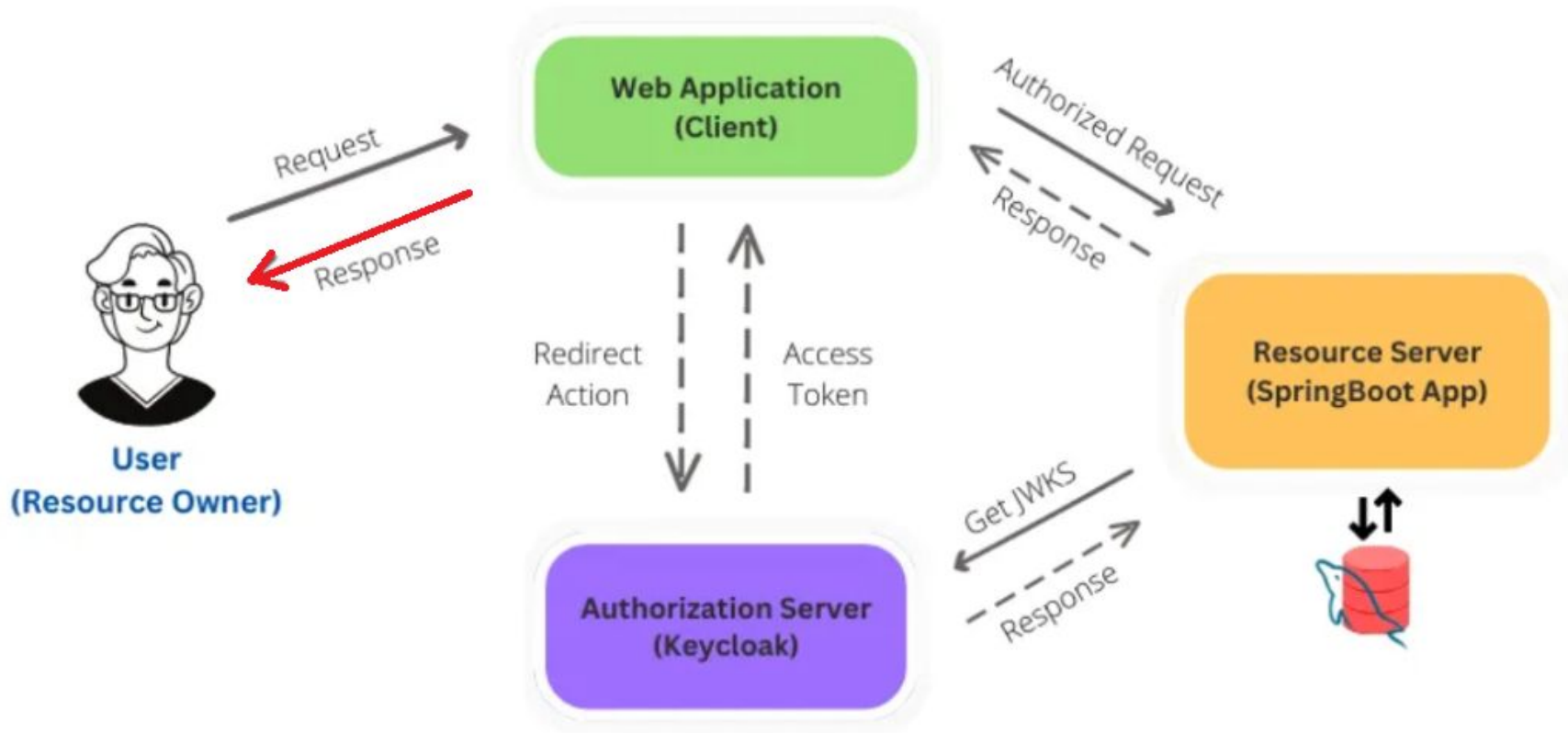
FLUXO



FLUXO



FLUXO



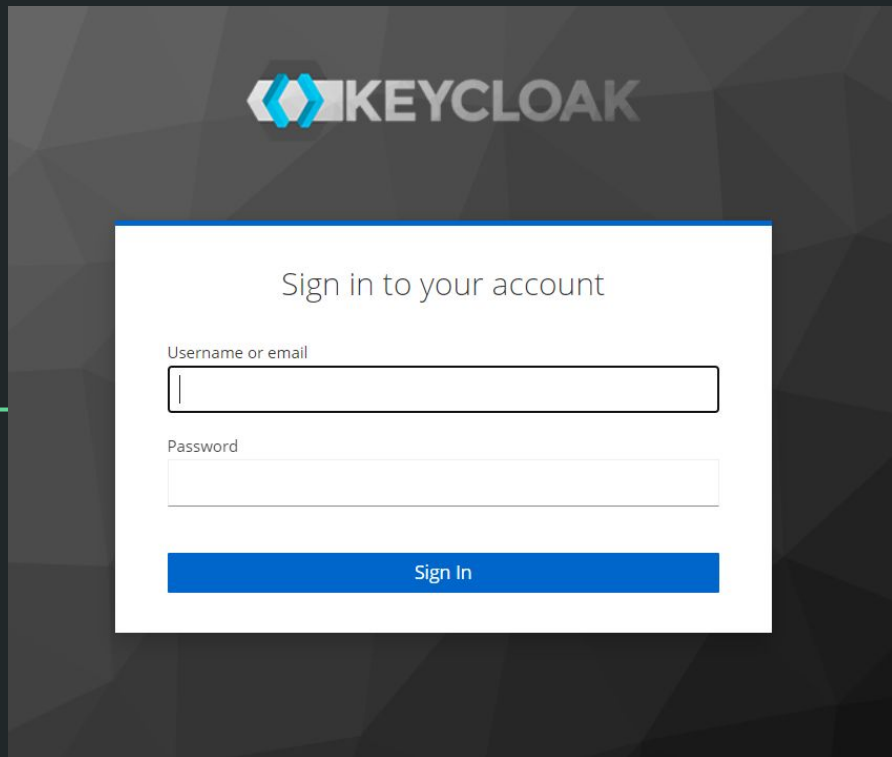
IMPLEMENTAÇÃO

CRIANDO CONTAINER

```
C:\Users\danub>docker run -p 8080:8080 -e KEYCLOAK_ADMIN=admin -e KEYCLOAK_ADMIN_PASSWORD=admin  
quay.io/keycloak/keycloak:21.1.1 start-dev|
```

IMPLEMENTAÇÃO

ACESSANDO



The image shows the Keycloak login interface. At the top center is the Keycloak logo, which consists of a blue and white geometric icon followed by the word "KEYCLOAK" in a bold, sans-serif font. Below the logo, the text "Sign in to your account" is centered. Underneath this text are two input fields: the first is labeled "Username or email" and the second is labeled "Password". Both fields are empty and have a thin border. At the bottom of the form is a blue button with the text "Sign In" in white. The entire form is set against a dark gray background with a subtle geometric pattern.

KEYCLOAK

Sign in to your account

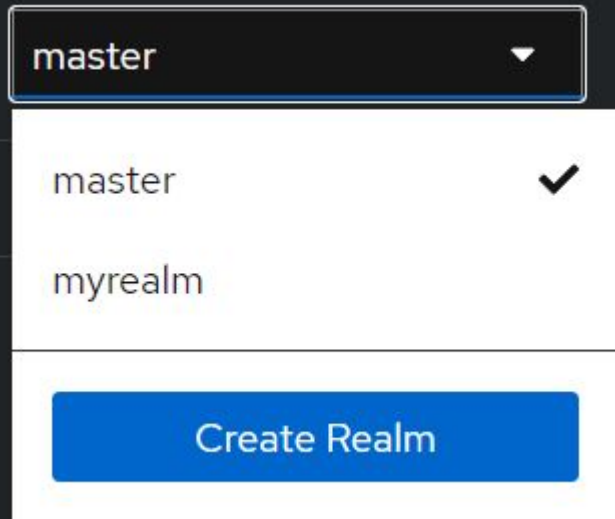
Username or email

Password

Sign In

IMPLEMENTAÇÃO

CRIANDO UM REALM



master

master ✓

myrealm

Create Realm

“ É uma unidade de isolamento e gerenciamento de usuários, identidades e políticas de segurança “

IMPLEMENTAÇÃO

CLIENTS

Clients

Clients are applications and services that can request authentication of a user. [Learn more](#)

Clients list

Initial access token

Client registration

Q Search for client

→

Create client

Import client

1-7 < >


Client ID	Name	Type	Description	Home URL	
MYCLIENT	–	OpenID Connect	–	–	⋮
account	\${client_account}	OpenID Connect	–	http://localhost:8080/realms/myrealm/account/	⋮
account-console	\${client_account-console}	OpenID Connect	–	http://localhost:8080/realms/myrealm/account/	⋮
admin-cli	\${client_admin-cli}	OpenID Connect	–	–	⋮
broker	\${client_broker}	OpenID Connect	–	–	⋮
realm-management	\${client_realm-manageme...}	OpenID Connect	–	–	⋮
security-admin-console	\${client_security-admin-c...}	OpenID Connect	–	http://localhost:8080/admin/myrealm/console/	⋮


1-7 < >



IMPLEMENTAÇÃO

Configurando seu Client

Access settings

Root URL 

Home URL 

Valid redirect URIs  

[+ Add valid redirect URIs](#)

Indicando URI do Client

IMPLEMENTAÇÃO

REGRAS DO CLIENT:

- São aplicadas em um nível específico do cliente (aplicação ou serviço) dentro de um realm.
 - Podem ser usadas para manipular os tokens de autenticação, adicionar informações extras nos tokens, aplicar regras de acesso, entre outras personalizações.
-

REGRAS DO REALM:

- Elas são usadas para adicionar lógica personalizada em todo o processo de autenticação e autorização para todos os clientes dentro de um realm.
- São definidas e gerenciadas no nível do realm e se aplicam a todos os clientes configurados dentro desse realm.

IMPLEMENTAÇÃO

Configurando seu Client

Create role

Role name *

Description

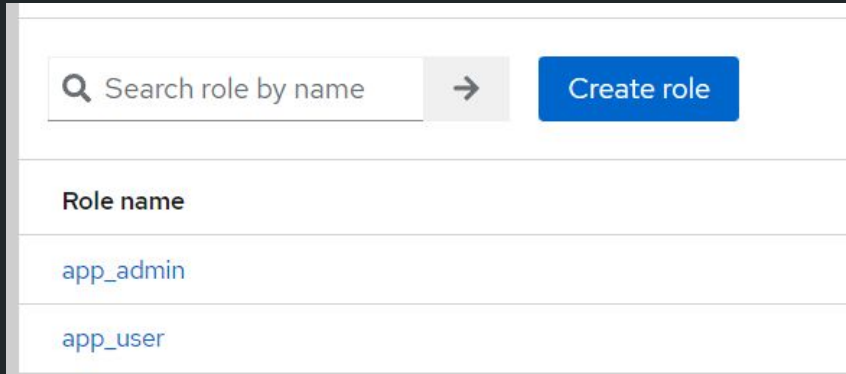
Criando Regras

<input type="text" value="Search role by name"/>	<input type="button" value="→"/>	<input type="button" value="Create role"/>
Role name	Composite	
admin	False	
user	False	

Regras Criadas

IMPLEMENTAÇÃO

Criando Regras para o Realm



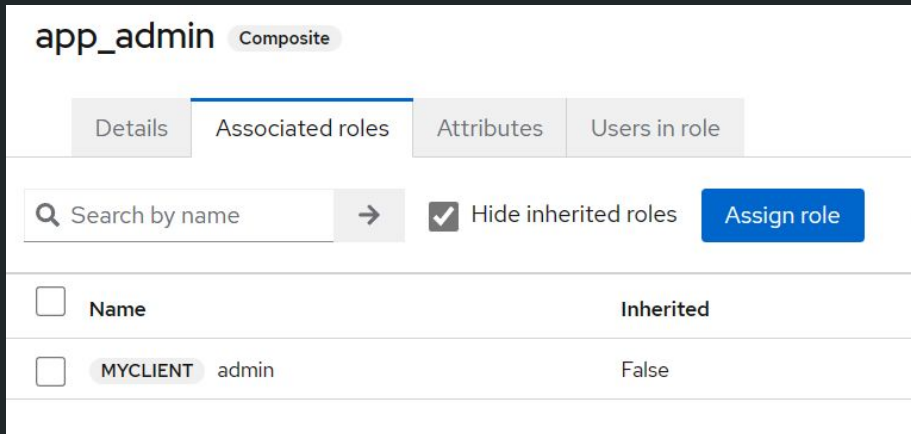
Search role by name → Create role

Role name

app_admin

app_user

Criando Role



app_admin Composite

Details Associated roles Attributes Users in role

Search by name → ☒ Hide inherited roles Assign role

<input type="checkbox"/> Name	Inherited
<input type="checkbox"/> MYCLIENT admin	False

Associando Role

IMPLEMENTAÇÃO

Criando Usuários

User list

→

Add user

Delete user

<input type="checkbox"/>	Username	Email
<input type="checkbox"/>	danadmin	! dubamacedoo@gmail.com
<input type="checkbox"/>	danuser	! danubiatestes@gmail.com

IMPLEMENTAÇÃO

Credenciais do Usuário

danadmin

Enabled

Action ▾

Details

Attributes

Credentials

Role mapping

Groups

Consents

Identity provider links

Sessions


?

Type

User label

Data

Password

My password 

Show data

Reset password

⋮

Credential Reset

IMPLEMENTAÇÃO

Adicionando Regras

Assign roles to danadmin

<input type="checkbox"/> Name	Description
<input type="checkbox"/> app_user	
<input type="checkbox"/> offline_access	\${role_offline-access}
<input type="checkbox"/> uma_authorization	

danadmin

Details Attributes Credentials Role mapping Groups Consents Identity provider links

☒ Hide inherited roles

<input type="checkbox"/> Name	Inherited	Description
<input type="checkbox"/> default-roles-myrealm	False	\${role_default-roles}
<input type="checkbox"/> app_admin	False	—

IMPLEMENTAÇÃO

JWT E ACCESS TOKEN

MYCLIENT OpenID Connect

Clients are applications and services that can request authentication of a user.

Settings

Keys

Credentials


Roles

Client scopes

Authorization

Service accounts roles

Sessi



Client Authenticator


Client Id and Secret

Save

Client secret

UI8RfxsTjHn6luPEoqYesEvxrE9LQSre



IMPLEMENTAÇÃO

JWT E ACCESS TOKEN

POST

http://localhost:8080/realms/myrealm/protocol/openid-connect/token

Params

Authorization

Headers (8)

Body

Pre-request Script

Tests

Settings

☐ none

☐ form-data

☒ x-www-form-urlencoded

☐ raw

☐ binary

☐ GraphQL

	KEY	VALUE
<input checked="" type="checkbox"/>	client_id	MYCLIENT
<input checked="" type="checkbox"/>	client_secret	UI8RfxsTjHn61uPEoqYesEvxrE9LQSre
<input checked="" type="checkbox"/>	grant_type	password
<input checked="" type="checkbox"/>	password	danadmin
<input checked="" type="checkbox"/>	username	danadmin

JWT E ACCESS TOKEN

JWT.IO



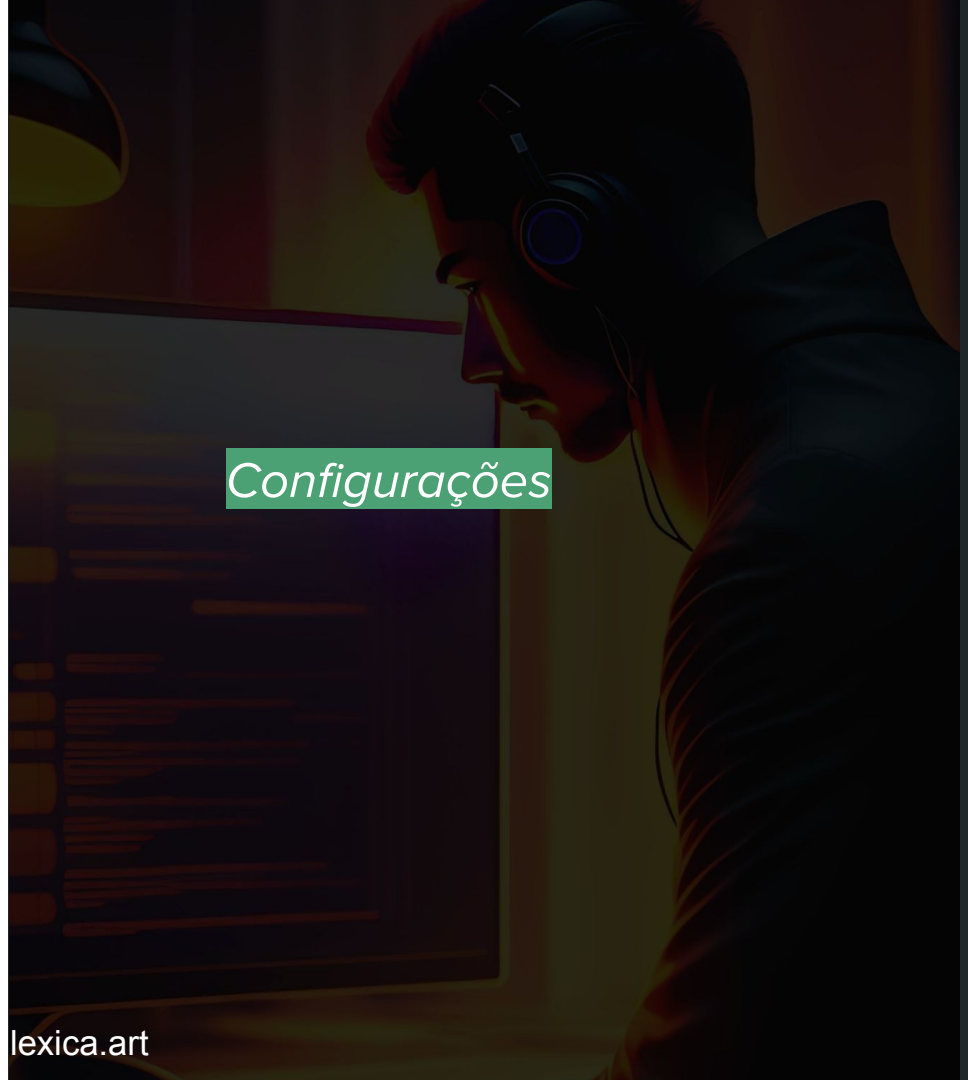
IMPLEMENTAÇÃO

```
{
  "exp": 1685925301,
  "iat": 1685925001,
  "jti": "bbbc0db6-7a0a-4705-a630-e86930080fb6",
  "iss": "http://localhost:8080/realms/myrealm",
  "aud": "account",
  "sub": "7960e831-aeb4-4eee-bd7c-123ecd7afa61",
  "typ": "Bearer",
  "azp": "MYCLIENT",
  "session_state": "78ce81e9-31d0-4069-8283-
e2ae6cca7a3c",
  "acr": "1",
  "allowed-origins": [
    "https://www.keycloak.org/"
  ],
  "realm_access": {
    "roles": [
      "default-roles-myrealm",
      "offline_access",
      "uma_authorization",
      "app_admin"
    ]
  },
  "resource_access": {
    "MYCLIENT": {
      "roles": [
        "admin"
      ]
    }
  },
}
```

```
},
"account": {
  "roles": [
    "manage-account",
    "manage-account-links",
    "view-profile"
  ]
},
"scope": "email profile",
"sid": "78ce81e9-31d0-4069-8283-e2ae6cca7a3c",
"email_verified": false,
"name": "dan admin dan",
"preferred_username": "danadmin",
"given_name": "dan admin",
"family_name": "dan",
"email": "dubamacedoo@gmail.com"
}
```


Spring Framework e Spring Security

Configurações



Configurações no Spring

application.yml

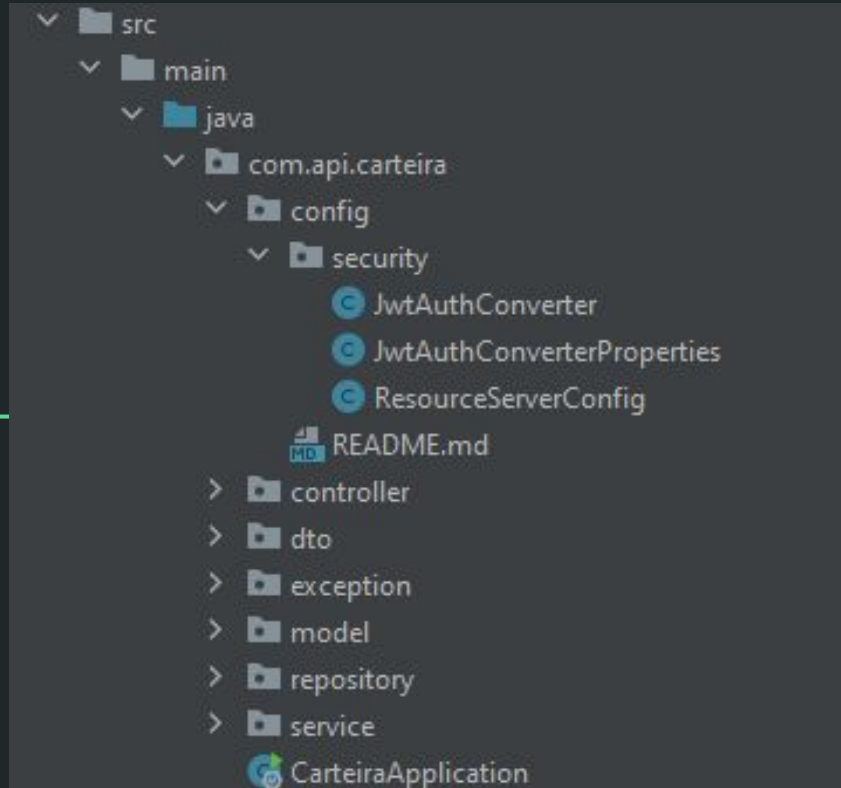
```
spring:
  application:
    name: MYREALM
  security:
    oauth2:
      resourceserver:
        jwt:
          issuer-uri: http://localhost:8080/realms/myrealm
          jwk-set-uri: ${spring.security.oauth2.resourceserver.jwt.issuer-uri}/protocol/openid-connect/certs

  jwt:
    auth:
      converter:
        resource-id: MYCLIENT
        principal-attribute: preferred_username

logging:
  level:
    org.springframework.security: DEBUG
```

Configurações no Spring

Arquivos de Configuração Spring Security



Configurações no Spring

Autorização

```
@Bean
public SecurityFilterChain securityFilterChain(HttpSecurity http) throws Exception {

    http.authorizeHttpRequests()
        .requestMatchers(HttpMethod.GET, ...patterns: "/wallet").hasRole(ADMIN)
        .anyRequest().authenticated();

    http.oauth2ResourceServer()
        .jwt()
        .jwtAuthenticationConverter(jwtAuthConverter);
    http.sessionManagement().sessionCreationPolicy(SessionCreationPolicy.STATELESS);
    return http.build();
}
```

API CARTEIRA

Cadastrar

Listar Todos

Editar

Buscar por ativo específico

Deletar

Buscar Histórico de Preço

Autenticação

Params **Authorization** Headers (9) Body Pre-request Script Tests Settings

Type

Bearer Token



The authorization header will be automatically generated when you send the request.

[Learn more about authorization](#)



Heads up! These parameters hold sensitive data. To keep this data secure while working in a collabora

Token

eyJhbGciOiJSUzI1NiIsInR5cCI6ImlzdiUliwi...

Cadastrar

POST

localhost:8082/wallet

Params

Authorization ●

Headers (9)

Body ●

☐ none

☒ form-data

☐ x-www-form-urlencoded


```
1  {  
2    "ticker": "BBAS3.SA",  
3    "tipo": "ACA0",  
4    "percentualAlocacao": "10",  
5    "precoTeto": "10000"  
6  }
```





Status: 200 OK Time: 123 ms Size: 293 B

Save Response ▾

Buscar Todos

GET  localhost:8082/wallet?page=0


Params  **Authorization**  **Headers (7)** **Body** **Pre-req**

Query Params


	KEY	VALUE
<input checked="" type="checkbox"/>	page	0
	Key	Value

```
"content": [  
  {  
    "ticker": "PETR3",  
    "tipo": "ACA0",  
    "percentualAlocacao": 5.5,  
    "precoTeto": 1000.0,  
    "uuid": "44f9732b-00f7-4547-8b38-0ac84f5eac93"  
  },  
  {  
    "ticker": "BBAS3.SA",  
    "tipo": "ACA0",  
    "percentualAlocacao": 10.0,  
    "precoTeto": 10000.0,  
    "uuid": "bdb3fd94-0cd8-4ddc-b9a9-3afafed8953a"  
  }  
],  
"pageable": {  
  "sort": {  
    "empty": true,  
    "sorted": false,  
    "unsorted": true  
  },  
  "offset": 0
```



Editar

PUT  localhost:8082/wallet

Params

Authorization 

Headers (9)

Body 


☐ none

☒ form-data

☐ x-www-form-urlencoded

```
1  {
2    "ticker": "PETR3",
3    "tipo": "ACAO",
4    "percentualAlocacao": "5.5",
5    "precoTeto": "1000"
6  }
```

Deletar

DELETE  http://localhost:8082/wallet/PETR3

Buscar Histórico de Preço de um Ativo

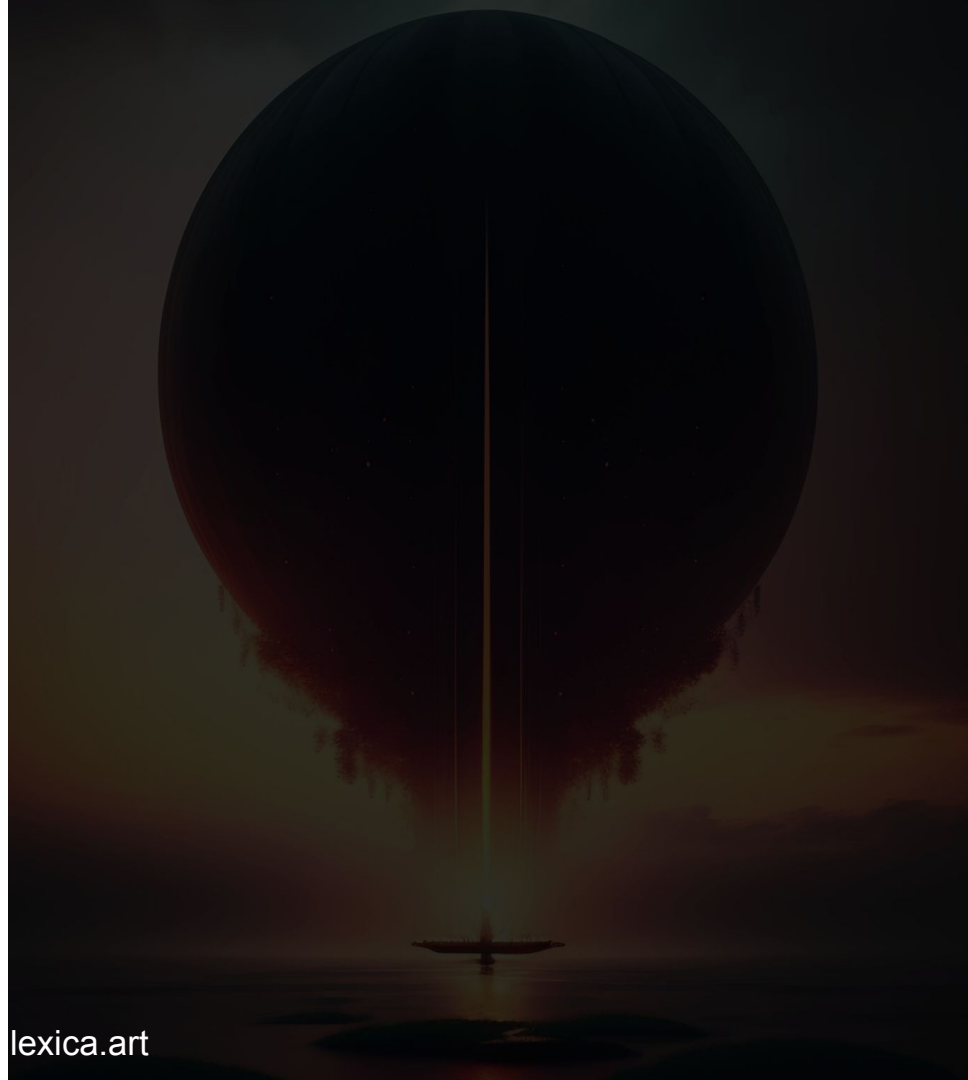
GET



<http://localhost:8082/wallet/buscarHistorico/BBAS3.SA>

CONCLUSÃO

Fonte: [lexica.art](https://www.lexica.art)

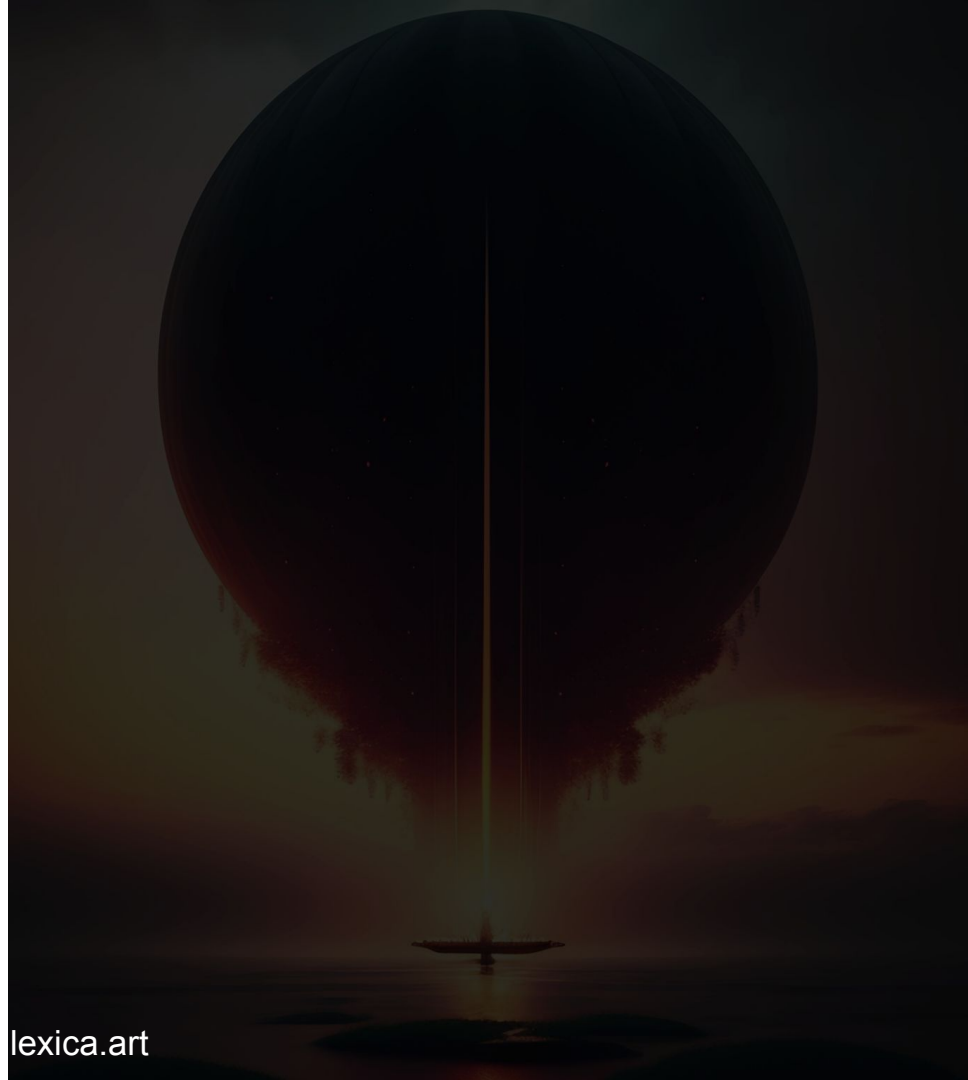


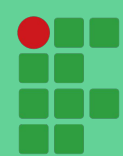
CONCLUSÃO

Em suma, o processo descrito anteriormente foi implementado para autenticar os usuários de nosso aplicativo de carteira financeira. Essa abordagem oferece uma segurança mais robusta para nossos clientes, juntamente com um controle de acesso flexível para gerenciar o acesso aos recursos do programa. Através da criação de níveis de acesso para usuários individuais ou grupos específicos, garantimos as permissões necessárias para que cada usuário possa executar suas tarefas. Além disso, o Keycloak nos permite centralizar a identidade, o que é crucial para uma gestão eficiente e simplificada.

CONSIDERAÇÕES

Fonte: [lexica.art](https://www.lexica.art)





OBRIGADO(A)!

danubia.macedo@estudante.ifmt.edu.br

leonardo.queiroz@estudante.ifmt.edu.br

wigorernandes@gmail.com