MicroBank

API Documentation v1.0

Author: Ahmet ATAR

Table of Contents

1. Introduction

1.1 Overview of Microservice Architecture

This project is built using a microservice architecture to achieve scalability, flexibility, and maintainability. Each microservice in the system is designed around a specific business domain, allowing independent development, deployment, and scaling. Key features of this architecture include:

- **Service Autonomy**: Each microservice manages its own database and operates independently, ensuring data consistency and reducing dependencies.
- **API Gateway**: A centralized gateway handles all incoming requests, routing them to the appropriate services and enforcing security measures such as authentication and authorization.
- **Event-Driven Communication**: The system leverages RabbitMQ for asynchronous communication between services, enabling real-time processing of particular events.
- **Containerized Approach**: Using Docker and Docker Compose, the system is packaged and deployed as containers, ensuring consistency across environments and simplifying scaling.

1.2 Purpose of Documentation

The purpose of this documentation is to provide a comprehensive guide for understanding, deploying, and interacting with the backend system. Specifically, this document aims to:

- Describe the system architecture and its components in detail.
- Provide setup instructions to get the system running in local or production environments.
- Offer detailed API references for developers to integrate and test the backend services.
- Encourage contributions by offering clear guidance on how developers can extend or improve the system.

This documentation is designed to facilitate both understanding and collaboration, making it easier to utilize and contribute to the project.

1.3 Target Audience

This documentation is intended for two main groups of people:

- **Developers who want to utilize the project**: Frontend and mobile developers looking to integrate with the backend system. This documentation provides clear guidance on how to interact with the APIs and leverage the system's functionality.
- **Developers who want to contribute to the project**: Backend developers or contributors interested in enhancing or extending the system. The documentation explains the architecture and internal workings to make contributing as seamless as possible.

Whether you're here to use the system or to contribute to its growth, this documentation is written to support your goals and make working with the project as straightforward as possible.

2. Getting Started

This section provides all the necessary information to set up and begin using the backend system. By following these steps, developers and testers can ensure they have the required tools and configuration to interact with the API seamlessly.

2.1 Prerequisites

Before you start using or deploying this project, ensure that the following prerequisites are met:

- Java 17 or higher for running the backend services.
- Maven (latest version) for building the microservices.
- Docker and Docker Compose for containerization and orchestration.
- Postman, Apidog, or any similar REST client for testing API endpoints.

2.2 Base URL Structure

The API is structured around a central API Gateway, which routes requests to the appropriate backend microservices. Below is the base URL structure for the API:

- **Base URL**: `http://localhost:8123/api/v1` (default for local environments)
- **Common Endpoint Patterns**:
  - `/auth/**` – Authentication-related endpoints (e.g., register, activate, login, password reset).
  - `/accounts/**` – User account operations (e.g., account creation, balance inquiries).
  - `/transactions/**` – Financial transaction operations (e.g., transfers).
  - `/documents/**` – Document-related operations (e.g., generating and downloading transaction receipts).
  - `/notifications/**` – Email notifications (e.g., account activation, transaction receipt information).

For production environments, replace `localhost` with the public domain or IP address of the deployment server.

2.3 Postman Collection

To simplify testing and interaction with the API, a Postman Collection has been provided as part of this project. The collection includes pre-configured requests for all microservice endpoints, along with example payloads and headers. Follow these steps to import and use the collection:

1. Download the Postman Collection from the root directory of the project repository (in the `./postman` directory):
2. Open Postman and import the collection:
   - Go to File > Import in Postman and select the JSON file.
3. Set up environment variables in Postman:
   - Add variables like `baseURL` with the value `http://localhost:8123/api/v1` and authentication tokens for seamless testing.
4. Test endpoints:
   - Use the imported collection to test endpoints across Authentication, Account, Transaction, Document, and Notification services.

This collection allows developers to quickly interact with the API without manually configuring requests, making the testing process streamlined and efficient.

2.4 Keycloak Realm Export

To simplify the setup of Keycloak for this project, a pre-configured `realm-export.json` file has been provided. This file includes all the necessary configurations, roles, and permissions to get started quickly with authentication and authorization. Using this file, you can import the realm into your Keycloak instance without manually creating roles or configuring client settings.

Steps to Import the Keycloak Realm Export:

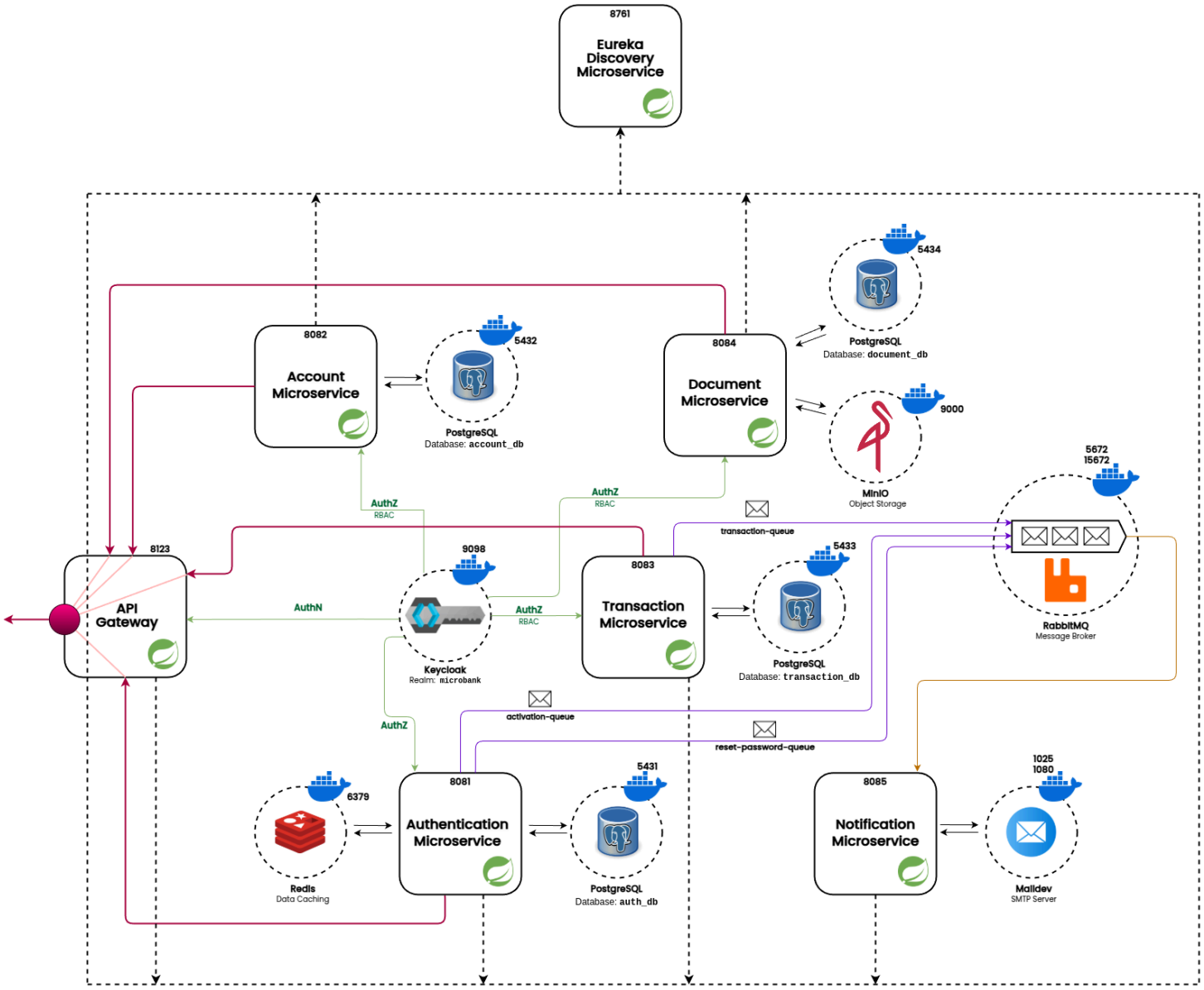
1. **Access Keycloak Admin Console**:
   - Open your browser and navigate to the Keycloak Admin Console.
   - Default URL for local setup: `http://localhost:9098.`
2. **Login to Admin Console**:
   - Use the administrator credentials set during Keycloak setup. (both username and password is **`admin`**)
3. **Import the Realm**:
   - Go to the "Realm Settings" section in the admin console.
   - Click on "Add Realm" and select the `realm-export.json` file provided in the repository.
   - You can find the `realm-export.json` file at the root project repository (in the **`./keycloak-config`** directory).
   - NOTE: You do not have to manually import the realm anymore, the Keycloak image in the Docker Compose file is configured so that the realm export JSON file is automatically being imported as the `microbank` realm.
4. **Test the Configuration**:
   - Use the credentials for test users or create new users in the realm and assign appropriate roles.

3. Project Architecture

The backend architecture of this project is based on the microservices paradigm, which ensures scalability, maintainability, and fault tolerance. Each microservice is responsible for a specific domain or functionality, and the overall architecture leverages cutting-edge technologies such as Docker, RabbitMQ, PostgreSQL, Redis, Keycloak, and MinIO. Below, a detailed breakdown of the project architecture is provided.

3.1 Backend Project Diagram

The system architecture revolves around several independent microservices that are orchestrated and interconnected via an API Gateway. The diagram outlines how these services communicate with each other and external systems. Central components include service discovery, authentication, database integration, message queues, and object storage.



3.2 Microservices of the Project

Each microservice in this project is independently deployable and designed around a specific business capability. These services work together to deliver the functionality of the platform while adhering to core principles of microservice architecture. Key highlights include:

- **Loose Coupling**: Services communicate primarily through HTTP/REST APIs and message queues, minimizing dependencies and enabling flexibility in service updates.

- **Autonomy**: Each service manages its own database, ensuring data isolation and reducing the risk of cross-service data corruption.
- **Scalability**: Microservices can be scaled independently based on workload and performance requirements, ensuring efficient resource utilization.

The core microservices and infrastructure components in this project are:

- **API Gateway**: The API Gateway acts as the single entry point for all client interactions. It efficiently routes requests to the appropriate backend microservices while handling authentication and authorization. By integrating with Keycloak, the gateway ensures secure authentication and token validation before forwarding requests. It also simplifies external access by abstracting the internal microservices' architecture, providing a unified API interface for clients.
- **Eureka Discovery Service**: Eureka serves as the backbone of service discovery and registration in this microservice ecosystem. It allows each microservice to register itself dynamically at runtime, enabling discovery of service endpoints. This eliminates the need for hardcoded service URLs and ensures load balancing. By leveraging Eureka, the architecture supports dynamic scaling, making it possible to deploy additional instances of any microservice.
- **Authentication Service**: The Authentication Service is the cornerstone of identity and access management in the system, working closely with Keycloak for token issuance and validation. It provides core functionalities such as user registration, login, account activation, and password recovery. To enhance performance, it utilizes Redis as a caching layer for temporary data. Its tight integration with the API Gateway and Keycloak ensures robust security and streamlined authentication workflows.
- **Account Service**: The Account Service is responsible for managing user account operations, including account creation, retrieval, and updates. It uses PostgreSQL for persistent data storage, ensuring data integrity and consistency. By enforcing role-based access control through Keycloak, it ensures that only authorized users can access or modify account information. As a core business microservice, it is accessible through the API Gateway, allowing external clients to perform account-related actions securely.
- **Transaction Service**: The Transaction Service handles the platform's financial operations, including processing transfers, payments, and deposits. It uses PostgreSQL for storing transaction records and maintains a robust audit trail. By publishing transaction events to the transaction queue in RabbitMQ, it supports asynchronous communication with the Notification Service.
- **Document Service**: The Document Service focuses on generating, storing, and delivering documents such as receipts, account statements, and transaction reports. Using Apache PDFBox, it dynamically creates PDF documents, which are then stored in MinIO. This microservice also utilizes PostgreSQL for metadata storage to retrieve and manage documents. By providing secure pre-signed URLs, the service ensures that users can access their documents safely.
- **Notification Service**: The Notification Service operates as an internal microservice dedicated to sending email notifications based on events occurring within the system. It consumes messages from RabbitMQ queues such as transaction, account activation, and password recovery messages, ensuring event-driven communication and real-time notification delivery. Emails are sent using MailDev which is an SMTP server. By remaining internal and not directly accessible through the API Gateway, this service enhances system security while efficiently handling event-driven notification workflows.

3.3 Storage Solutions

This project uses several stateful components, each tailored to its purpose, all deployed via Docker containers for consistent and isolated environments:

- **PostgreSQL**:
  - Used for persistent, relational data storage across microservices.
  - Each service (Authentication, Account, Transaction, Document) maintains its own PostgreSQL instance with service-specific schemas.
- **Redis**:
  - Serves as a high-speed, in-memory cache for temporary data such as user data with activation codes in registration process, and password recovery codes when users forgot their password.
  - Accelerates the performance of the Authentication Service by reducing frequent database hits and serves as a data bridge in user registration.
- **MinIO**:
  - Acts as an object storage solution for the Document Service.
  - Stores user-generated receipts related to particular transactions in a scalable, S3-compatible storage layer.
  - Files are accessed via pre-signed URLs, ensuring secure delivery to clients.

These solutions are configured to run as containerized services, ensuring seamless integration with the rest of the system.

3.4 Containerization

The entire backend infrastructure is containerized using Docker, which ensures consistency across development, testing, and production environments. Key components include:

- **Docker Images**:
  - Microservices and dependencies (e.g., Keycloak, RabbitMQ, PostgreSQL, Redis, MailDev, MinIO) are deployed as Docker images.
  - Services are isolated yet interoperable within the same Docker network.
- **Docker Compose**:
  - A `docker-compose.yml` file orchestrates the startup of all external services.
  - Ensures that all containers, including infrastructure services like RabbitMQ and MinIO, are launched in the correct order.
  - Simplifies local development and testing by allowing the entire system to be brought up with a single command.

This approach accelerates deployment, facilitates scaling, and ensures reproducibility across environments.

3.5 Service Communications

The project employs a hybrid communication model for inter-service interactions, balancing performance and reliability:

- **Asynchronous Communication**:
  - RabbitMQ is utilized for event-driven messaging between services.
  - Key queues include:
    - `activation-queue:` Handles user activation events.
    - `reset-password-queue:` Processes password reset requests.
    - `transaction-queue:` Publishes transaction events for downstream services.
  - This asynchronous approach decouples services, enabling them to operate independently and improving system resiliency.
- **Synchronous Communication**:
  - Microservices interact synchronously via HTTP calls using Spring Cloud OpenFeign.
  - OpenFeign simplifies REST client creation and supports load balancing and fault tolerance via Eureka Service Discovery.

4. Identity and Access Management

This section covers the answer of the questions how the MicroBank backend is being protected and why those methods are used.

4.1 Keycloak Integration Overview

Keycloak serves as the central authentication and authorization provider for this project. Instead of implementing a custom authentication system, Keycloak offers out-of-the-box support for essential security features such as user authentication, role-based access control (RBAC), single sign-on (SSO), multi-factor authentication (MFA), and identity federation.

A pre-configured Keycloak realm named **`microbank`** is included in the project root directory as **`realm-export.json`**. This file allows developers to quickly set up Keycloak without manually creating users, roles, or clients.

Preconfigured Realm Features:

- **Realm Name:** `microbank`
- **User Roles:**
  - **USER** – Standard users with limited access.
  - **ADMIN** – Administrators with full control over the system.
- **Predefined Clients:**
  - **admin-cli** – Used for managing Keycloak configurations and user registrations.
  - **microbank-client** – Used by the backend services for authentication and authorization.
- **Client Credentials:**
  - The client ID and secret keys can be regenerated and updated in `application.yml` for each microservice.
- **Security Algorithms:**
  - Keycloak JWKs (JSON Web Keys) are encrypted using the RS256 signature algorithm, which is an asymmetric encryption mechanism that ensures high-security standards.

Keycloak supports multiple authentication and authorization protocols, including:

- **OAuth 2.0** – For API authentication and token-based authorization.
- **OpenID Connect (OIDC)** – A layer on top of OAuth 2.0, providing identity verification and user authentication.
- **SAML 2.0** – For single sign-on (SSO) integrations with enterprise identity providers.

These capabilities make Keycloak an ideal choice for securing modern microservice architectures.

IMPORTANT NOTE FOR ROLES: At the beginning of the project, there are no users, meaning there is no admin user either. Thus the first admin user should be registered as a regular user, then you should manually assign ADMIN roles in both Keycloak realm and Database (auth_db.users). There are two important points, though:

a. In the Keycloak realm, make sure you REASSIGN the USER role from this user before you ASSIGN the ADMIN role.

b. To access the PostgreSQL database (auth_db) and change the user's role, you can apply the following steps:

b.1. `psql -U auth_db -d auth_db -h localhost -p 5431` (access the database, password is "auth_db" as default)

b.2. `\dt` (make sure you have a table named "users")

b.3. `select * from users;` (see all data in the "users" table)

b.4. `update users set role = 'ADMIN' where role = 'USER';` (change the role of the user)

4.2 Authentication Protocol

The project follows the OAuth 2.0 Authorization Framework, using Keycloak as the authorization server. The API Gateway validates JWT tokens issued by Keycloak before forwarding requests to internal microservices.

Authentication Flow:

1. **User Registration & Login:**
   - Users register via the `/api/v1/auth/register` endpoint.
   - After successful registration, users activate their accounts via `/api/v1/auth/activate`.
   - Users log in via `/api/v1/auth/login`, and Keycloak issues a JWT (JSON Web Token).
2. **Token Validation & API Access:**
   - The API Gateway verifies the JWT token and extracts user roles and permissions.
   - If the token is valid, the request is forwarded to the respective microservice.
   - If the token is invalid or expired, the request is rejected with a `401 Unauthorized` response.
3. **Role-Based Access Control (RBAC):**
   - **Keycloak roles** (`USER, ADMIN`) are mapped to Spring Security authorities (`ROLE_USER, ROLE_ADMIN`).
   - Microservices enforce authorization using Spring Security annotations or path-based access control.

The authentication mechanism relies on OAuth 2.0 Bearer Tokens, which are included in the `Authorization` header of each request:

```
Authorization: Bearer <JWT>
```

JWT tokens contain user claims, including roles, which are used for authorization at the microservice level.

4.3 Web Security and Web Flux Security

The project separates authentication (AuthN) from authorization (AuthZ) by implementing Spring Security differently in the API Gateway and microservices.

4.3.1 API Gateway (AuthN Layer)

- The API Gateway is reactive and built using Spring WebFlux.
- Reactive security mechanisms are required, so `@EnableWebFluxSecurity` is used instead of `@EnableWebSecurity`.
- Security is configured via `SecurityWebFilterChain:`

The security configuration of the API Gateway Service is constructed as follows:

```
@Configuration
@EnableWebFluxSecurity
@EnableReactiveMethodSecurity
public class SecurityConfig {

    @Value("${...}")
    private String issuerUri;
```

```
    @Bean
    public SecurityWebFilterChain securityWebFilterChain(ServerHttpSecurity serverHttpSecurity) {
        return serverHttpSecurity
                .csrf(ServerHttpSecurity.CsrfSpec::disable)
                .authorizeExchange(auth -> auth
                        .pathMatchers(HttpMethod.POST,  "/api/v1/auth/register").permitAll()
                        .pathMatchers(HttpMethod.POST,  "/api/v1/auth/activate").permitAll()
                        .pathMatchers(HttpMethod.POST,  "/api/v1/auth/login").permitAll()
                        .pathMatchers(HttpMethod.POST,  "/api/v1/auth/refresh-token").permitAll()
                        .pathMatchers(HttpMethod.POST,  "/api/v1/auth/forgot-password").permitAll()
                        .pathMatchers(HttpMethod.PATCH, "/api/v1/auth/reset-password").permitAll()
                        .anyExchange().authenticated()
                )
                .oauth2ResourceServer(oauth2 -> oauth2.jwt(jwt ->
                        jwt.jwtDecoder(ReactiveJwtDecoders.fromIssuerLocation(issuerUri))
                ))
                .build();
    }

}
```

The API Gateway:

- Authenticates all incoming requests using JWT tokens.
- Forwards only authenticated requests to microservices.
- Rejects unauthorized access attempts at the gateway level.

4.3.2 Microservices (Authorization Layer)

- Each microservice is stateful and uses Spring MVC (non-reactive security).
- Standard `@EnableWebSecurity` and `HttpSecurity` are used instead of reactive security.
- Security is configured via `SecurityFilterChain`:

The security configuration of other microservices is constructed as follows:

```
@Configuration
@EnableWebSecurity
public class SecurityConfig {

    @Value("${...}")
    private String jwkSetUri;

    @Bean
    public SecurityFilterChain securityFilterChain(HttpSecurity httpSecurity) throws Exception {
        return httpSecurity
              .csrf(AbstractHttpConfigurer::disable)
              .authorizeHttpRequests(auth -> auth
                    .requestMatchers(HttpMethod.POST,  "/api/v1/accounts").hasRole("USER")
                    .requestMatchers(HttpMethod.PUT,   "/api/v1/accounts/accounts/balance").hasRole("USER")
                    .requestMatchers(HttpMethod.GET,   "/api/v1/accounts").hasRole("USER")
                    .requestMatchers(HttpMethod.GET,   "/api/v1/accounts/{accountId}").hasRole("USER")
                    .requestMatchers(HttpMethod.DELETE,"/api/v1/accounts/{accountId}").hasRole("USER")

                    .requestMatchers(HttpMethod.GET,   "/api/v1/accounts/{accountId}/iban").hasRole("USER")
                    .requestMatchers(HttpMethod.GET,   "/api/v1/accounts/iban/{iban}").hasRole("USER")

                    .requestMatchers(HttpMethod.GET,   "/api/v1/admin/accounts").hasRole("ADMIN")
                    .requestMatchers(HttpMethod.GET,   "/api/v1/admin/accounts/{accountId}").hasRole("ADMIN")
                    .requestMatchers(HttpMethod.GET,   "/api/v1/admin/users/{userId}/accounts").hasRole("ADMIN")
                    .requestMatchers(HttpMethod.PATCH, "/api/v1/admin/accounts{accountId}/status").hasRole("ADMIN")
                    .requestMatchers(HttpMethod.DELETE,"/api/v1/admin/accounts/{accountId}").hasRole("ADMIN")

                    // Feign Permissions
                    .requestMatchers(HttpMethod.GET,   "/api/v1/auth/users/me").hasRole("USER")
                    .requestMatchers(HttpMethod.GET,   "/api/v1/auth/admin/users/{userId}").hasRole("ADMIN")

                    .anyRequest().authenticated()
              )
              .oauth2ResourceServer(oauth2 -> oauth2
                      .jwt(jwt -> jwt.jwtAuthenticationConverter(jwtAuthConverter()))
              )
              .build();
    }

    @Bean
    public JwtDecoder jwtDecoder() {
        return NimbusJwtDecoder.withJwkSetUri(jwkSetUri).build();
```

```
    }

    @Bean
    public JwtAuthenticationConverter jwtAuthConverter() {
        JwtAuthenticationConverter converter = new JwtAuthenticationConverter();
        converter.setJwtGrantedAuthoritiesConverter(new KeycloakRoleConverter());
        return converter;
    }
}



public class KeycloakRoleConverter implements Converter<Jwt, Collection<GrantedAuthority>> {

    @Override
    public Collection<GrantedAuthority> convert(@NonNull Jwt jwt) {
        Collection<GrantedAuthority> defaultAuthorities = new JwtGrantedAuthoritiesConverter().convert(jwt);

        List<String> realmRoles = extractRealmRoles(jwt);

        return Stream.concat(
                        defaultAuthorities.stream(),
                        realmRoles.stream()
                                .map(role -> new SimpleGrantedAuthority("ROLE_" + role.toUpperCase()))
                )
                .collect(Collectors.toSet());
    }

    private List<String> extractRealmRoles(Jwt jwt) {
        Map<String, Object> realmAccess = jwt.getClaim("realm_access");

        if (realmAccess == null || ObjectUtils.isEmpty(realmAccess.get("roles"))) {
            return List.of();
        }

        return (List<String>) realmAccess.get("roles");
    }
}
```

Microservices:

- Authorize requests based on user roles extracted from JWT tokens.
- Apply fine-grained authorization at the service level.
- Convert JWT roles into Spring Security authorities using `JwtAuthenticationConverter`.

4.3.3 Why WebFlux Security for API Gateway?

- The API Gateway is reactive, built using Spring WebFlux.
- Spring WebFlux does not support traditional `HttpSecurity`, so `ServerHttpSecurity` is required.
- API Gateway security must be non-blocking and fully asynchronous, which is why reactive security (WebFlux) is required.

4.3.4 Why Traditional Web Security for Microservices?

- Microservices handle business logic and persistent data, which work best with Spring MVC.
- Since microservices are not fully reactive, blocking security mechanisms (`HttpSecurity`) work better.
- Stateful authorization mechanisms are easier to manage in non-reactive microservices.

5. Endpoints Overview

Function Name	Method	Endpoint URL	AuthZ
Register User	**POST**	/api/v1/auth/register	**Public**
Activate User	**PATCH**	/api/v1/auth/activate	**Public**
Login User	**POST**	/api/v1/auth/login	**Public**
Refresh Token	**POST**	/api/v1/auth/refresh-token	**Public**
Forgot Password	**POST**	/api/v1/auth/forgot-password	**Public**
Reset Password	**PATCH**	/api/v1/auth/reset-password	**Public**

Get Current User's Profile	`GET`	`/api/v1/auth/users/me`	`USER`
Get User by ID	`GET`	`/api/v1/auth/admin/users/{userId}`	`ADMIN`
Get All Users	`GET`	`/api/v1/auth/admin/users`	`ADMIN`
Update User Role	`PATCH`	`/api/v1/auth/admin/users/role`	`ADMIN`
Update User Access	`PATCH`	`/api/v1/auth/admin/users/access`	`ADMIN`
Delete User	`DELETE`	`/api/v1/auth/admin/users/{userId}`	`ADMIN`
Create Bank Account	`POST`	`/api/v1/accounts`	`USER`
Update Account Balance	`PUT`	`/api/v1/accounts/balance`	`USER`
Get Current User's All Accounts	`GET`	`/api/v1/accounts`	`USER`
Get Current User's Account by ID	`GET`	`/api/v1/accounts/{accountId}`	`USER`
Get All Accounts	`GET`	`/api/v1/accounts/admin/accounts`	`ADMIN`
Get Account by ID	`GET`	`/api/v1/accounts/admin/accounts/{accountId}`	`ADMIN`
Get Accounts by User ID	`GET`	`/api/v1/accounts/admin/users/{userId}/accounts`	`ADMIN`
Update Account Status	`PATCH`	`/api/v1/accounts/admin/accounts/status`	`ADMIN`
Delete Own Account	`DELETE`	`/api/v1/accounts/{accountId}`	`USER`
Delete Account	`DELETE`	`/api/v1/accounts/admin/accounts/{accountId}`	`ADMIN`
Create Transaction	`POST`	`/api/v1/transactions`	`USER`
Get Current User's All Transactions	`GET`	`/api/v1/transactions/me`	`USER`
Get Current User's Transaction by ID	`GET`	`/api/v1/transactions/me/{transactionId}`	`USER`
Get Current User's Transactions by Account ID	`GET`	`/api/v1/transactions/me/accounts/{accountId}`	`USER`
Get All Transactions	`GET`	`/api/v1/transactions/admin/transactions`	`ADMIN`
Get Transactions by ID	`GET`	`/api/v1/transactions/admin/transactions/{transactionId}`	`ADMIN`
Get Transactions by Account ID	`GET`	`/api/v1/transactions/admin/accounts/{accountId}/transactions`	`ADMIN`
Get Transactions by User ID	`GET`	`/api/v1/transactions/admin/users/{userId}/transactions`	`ADMIN`
Get Transaction Document by ID	`GET`	`/api/v1/documents/{documentId}`	`USER`
Get Transaction Document by Transaction ID	`GET`	`/api/v1/documents/transactions/{transactionId}`	`USER`
Get All Transaction Documents	`GET`	`/api/v1/documents/admin/documents`	`ADMIN`

6. Standardized API Response Format

To ensure consistency and maintainability across all services in the MicroBank project, API responses follow a standardized format. Every successful and unsuccessful response adheres to a well-defined structure, enabling seamless integration for client applications and uniform error handling.

All endpoints are designed to respond in the same standardized format, ensuring a cohesive developer experience across the entire API. However, certain exceptions exist for **401 Unauthorized** and **403 Forbidden** errors directly related to authentication (AuthN) and authorization (AuthZ). In these cases, the API might not return a detailed response.

This structure is encapsulated in two key response classes:

- **`BaseApiResponse<T>:`** Used for successful API responses.
- **`ErrorResponse:`** Used for error handling and exception messages.

By standardizing API responses, client developers benefit from predictable response structures, improved error handling, and a streamlined integration process.

6.1. Base API Response Structure

The `BaseApiResponse<T>` class is a generic wrapper for all successful responses. It encapsulates essential response attributes such as status code, message, data, timestamp, and errors (if applicable).

Class Definition

```
public class BaseApiResponse<T> {

    private int status;
    private String message;
    private T data;
    private LocalDateTime timestamp;
    private List<String> errors;

    public BaseApiResponse() {
        this.timestamp = LocalDateTime.now();
    }

    public BaseApiResponse(int status, String message, T data) {
        this.status = status;
        this.message = message;
        this.data = data;
        this.timestamp = LocalDateTime.now();
        this.errors = null;
    }

    public BaseApiResponse(int status, String message, List<String> errors) {
        this.status = status;
        this.message = message;
        this.errors = errors;
        this.timestamp = LocalDateTime.now();
        this.data = null;
    }

    // Getters and Setters ...
}
```

Successful Response Example


```
{
    "status": 200,
    "message": "Role of user with ID: 24682698-9d9e-4e64-b046-2c34fd88f45a changed from USER to ADMIN successfully.",
    "data": {
        "id": "24682698-9d9e-4e64-b046-2c34fd88f45a",
        "keycloakId": "8c803a20-d28e-49fc-b5f3-4c763528b792",
        "username": "johndoe",
        "email": "john@email.com",
        "firstName": "John",
        "lastName": "Doe"
    },
    "timestamp": "2025-01-07T21:03:48.268136865",
    "errors": null
}
```


6.2. Error Response Structure and Special Cases

For handling errors and exceptions, the `ErrorResponse` class provides a structured approach to conveying error details to the client.

Class Definition

```
public class ErrorResponse {

    private int status;
    private String error;
    private String message;
    private List<String> details;
    private LocalDateTime timestamp;

    public ErrorResponse() {}

    public ErrorResponse(int status, String error, String message, List<String> details) {
        this.status = status;
        this.error = error;
        this.message = message;
        this.details = details;
        this.timestamp = LocalDateTime.now();
    }

    // Getters and Setters
}
```

Error Response Example

```
{
    "status": 400,
    "error": "Validation Error",
    "message": "Invalid request parameters",
    "details": [
        "Password must be at least 6 characters",
        "Invalid email format",
        "First name cannot be blank"
    ],
    "timestamp": "2025-01-07T20:56:02.594732937"
}
```

Special Case: AuthN and AuthZ Errors

For **401 Unauthorized** and **403 Forbidden** errors resulting from authentication or authorization issues (e.g., invalid tokens or insufficient permissions), the API does not return a detailed `BaseApiResponse`. Instead, the responses adhere to minimal error handling by returning standard HTTP status codes without additional details, aligning with security best practices.

Adopting a uniform API response format brings several advantages:

1. **Consistency**: Every response follows a predictable structure, reducing the learning curve for developers.
2. **Simplified Client Handling**: Frontend and mobile applications can process responses uniformly without handling multiple response formats.
3. **Better Debugging**: Detailed error responses make it easier to identify and resolve issues efficiently.
4. **Scalability**: As the project expands, new endpoints will automatically adhere to the same response structure.
5. **Security**: Specific error cases like **401 Unauthorized** and **403 Forbidden** responses might not be as detailed as other error responses.

By enforcing these standards, the MicroBank backend ensures a high level of reliability and maintainability for all API interactions.

7. Microservices

7.1 API Gateway Service

The API Gateway serves as the entry point for all external clients, including mobile and web applications. It routes requests to the appropriate microservices while handling authentication. By integrating with Keycloak, it ensures secure authentication and token validation. Additionally, it simplifies service discovery and communication by acting as a reverse proxy, allowing clients to interact with microservices without needing direct access to them.

As a matter of fact, the base URL of each microservice is distinct since they are separate backend projects and use different ports. For example:

- Authentication Microservice is running on port `8081` thus the base URL is `http://localhost:8081/api/v1,`
- Account Microservice is running on port `8082` thus the base URL is `http://localhost:8082/api/v1,`
- Transaction Microservice is running on port `8083` thus the base URL is `http://localhost:8083/api/v1,`
- Document Microservice is running on port `8084` thus the base URL is `http://localhost:8084/api/v1`

The base URL of the API Gateway is:

```
http://localhost:8123/api/v1
```

Every endpoint ready to be utilized by the client is available on this URL.

Eureka Discovery (`8761`) and Notification (`8085`) microservices are also running on a different port, Yet their endpoints are not being redirected to the API Gateway.

7.2 Eureka Discovery Service

The Eureka Discovery Service acts as a service registry, enabling dynamic registration and discovery of microservices. Instead of relying on static IP addresses or hardcoded service endpoints, microservices register themselves with Eureka, allowing them to discover and communicate with each other dynamically. This enhances fault tolerance and scalability, as services can be added or removed without requiring manual configuration updates.

7.3 Authentication Service

7.3.1 Register User `POST` `{baseURL}/auth/register`

Registers a new user and produces an activation code to be sent to the user's email address, caches the user data in the Redis along with the activation code for 15 minutes, tops, or till the user activates their account.

No path variable or header is required.

Request Body Field	Type	Mandatory
username	String	Yes
firstName	String	Yes
lastName	String	Yes
email	String	Yes
password	String	Yes

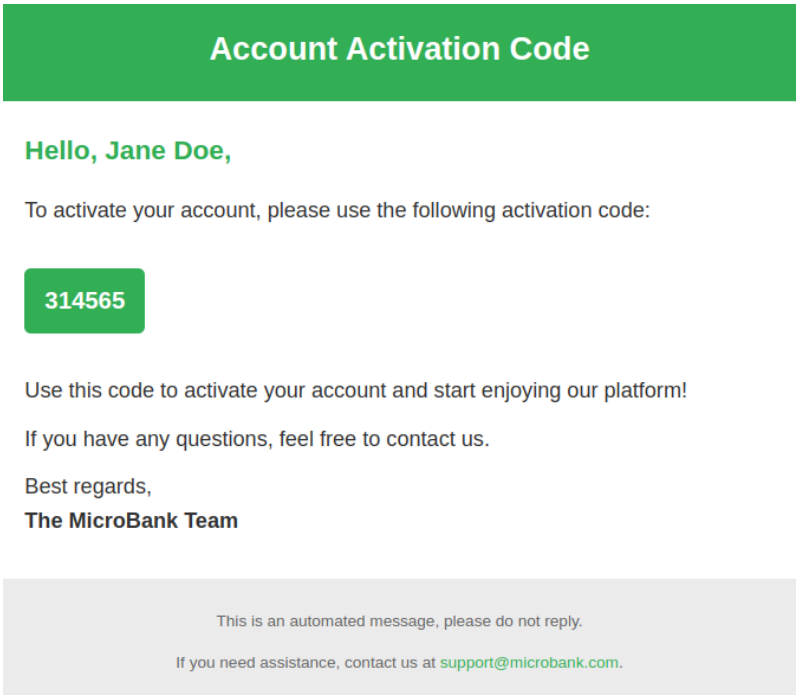
Example Request

```
{
    "username": "janedoe",
    "firstName": "Jane",
    "lastName": "Doe",
    "email": "jane@email.com",
    "password": "123456"
}
```

Example Response

```
{
    "status": 201,
    "message": "Registration successful, activation code sent to jane@email.com",
    "data": null,
    "timestamp": "2025-01-07T18:28:32.451676959",
    "errors": null
}
```

The provided email should receive an activation email template as follows:



7.3.2 Activate User `PATCH` `{baseURL}/auth/activate`

Activates the user's account, clears the cached user data and permanently saves it to the actual database, also completes the registration process in the Keycloak realm so Single Sign-On (SSO) can be effectively utilized across the permitted microservices.

No path variable or header is required.

Request Body Field	Type	Mandatory
email	String	Yes
activationCode	String	Yes

Example Request

```
{
    "email": "john@email.com",
    "activationCode": "314565"
}
```

Example Response

```
{
    "status": 200,
    "message": "Account activation successful, you can login to the system.",
    "data": null,
    "timestamp": "2025-01-07T18:29:37.713176044",
    "errors": null
}
```

7.3.3 Login User `POST` `{baseURL}/auth/login`

Users can log in to the system using this endpoint and get their access and refresh tokens. In MicroBank, users can access all authenticated endpoints, of course if they have an appropriate role, using the access token returned from this endpoint since Keycloak's Single Sign-On (SSO) support across the microservices.

No path variable or header is required.

Request Body Field	Type	Mandatory
username	String	Yes
password	String	Yes

Example Request

```
{
    "username": "johndoe",
    "password": "123456"
}
```

Example Response

```
{
    "status": 200,
    "message": "Login successful.",
    "data": {
        "access_token": "eyJhbGciOiJSUzI1NiIsInR5cCIgOiAiSldUIiwia2lkIiA6ICJNb3...",
        "expires_in": 300,
        "refresh_expires_in": 1800,
        "refresh_token": "eyJhbGciOiJIUzI1NiIsInR5cCIgOiAiSldUIiwia2lkIiA6ICIzY...",
        "token_type": "Bearer",
        "not-before-policy": 0,
        "session_state": "63a80ef9-7aeb-4362-a230-e20d523a11e2",
        "scope": "profile email"
    },
    "timestamp": "2025-01-07T19:43:08.889083057",
    "errors": null
}
```

7.3.4 Refresh Token `POST` `{baseURL}/auth/refresh-token`

Refreshes the user's access token using the refresh token. This feature can be utilized on the client side by setting up an automated token refreshing logic in order to keep user's session times longer.

No path variable or header is required.

Request Body Field	Type	Mandatory
refreshToken	String	Yes

Example Request

```
{
    "refreshToken": "eyJhbGciOiJIUzI1Ni..."
}
```

Example Response

```
{
    "status": 200,
    "message": "Token refreshed successfully.",
    "data": {
        "access_token": "eyJhbGciOiJSUzI1NiIsInR5cCIgOiAiSldU2lICJNb3...",
        "expires_in": 300,
        "refresh_expires_in": 1800,
        "refresh_token": "eyJhbGciOiJIUzI1NiIsInR5cCIgOiAiSldUIiwiIzY...",
        "token_type": "Bearer",
        "not-before-policy": 0,
        "session_state": "63a80ef9-7aeb-4362-a230-e20d523a11e2",
        "scope": "profile email"
    },
    "timestamp": "2025-01-07T19:43:08.889083057",
    "errors": null
}
```

7.3.5 Forgot Password `POST` `{baseURL}/auth/forgot-password`

Sends 6-digit password recovery code to the provided email address. In the next endpoint, this code is required to reset the user's password.

No path variable or header is required.

Request Body Field	Type	Mandatory
email	String	Yes

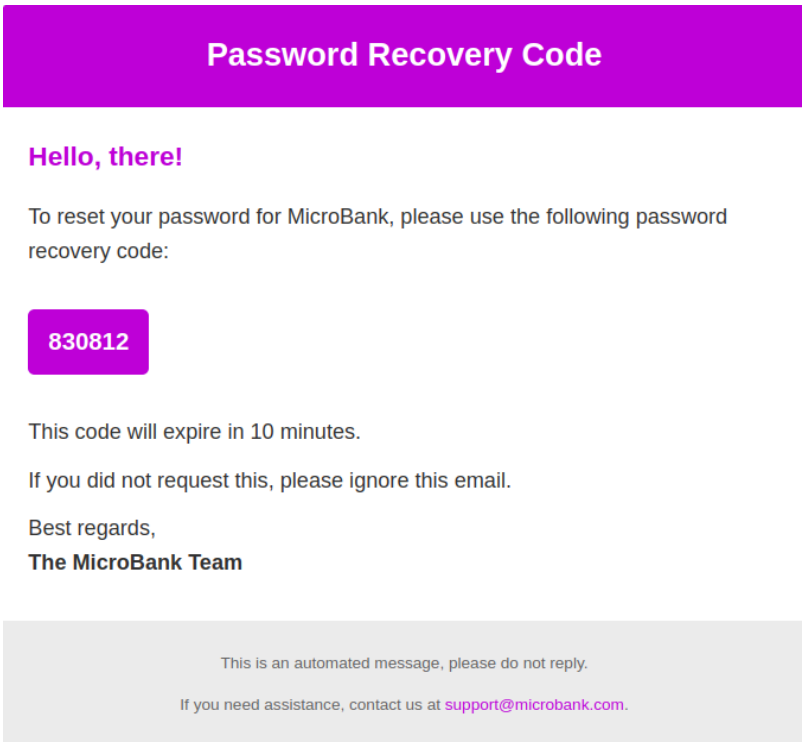
Example Request

```
{
    "email": "john@email.com"
}
```

Example Response

```
{
    "status": 200,
    "message": "Password recovery code sent to john@email.com",
    "data": null,
    "timestamp": "2025-01-07T19:43:08.889083057",
    "errors": null
}
```

The provided email should receive a password recovery email template as follows:



7.3.6 Reset Password `PATCH` `{baseURL}/auth/reset-password`

Resets the user's password using their email information as well as the 6-digit password recovery code that had been sent to their email addresses previously.

No path variable or header is required.

Request Body Field	Type	Mandatory
email	String	Yes
passwordRecoveryCode	String	Yes
newPassword	String	Yes

Example Request

```
{
    "email": "john@email.com",
    "passwordRecoveryCode": "830812",
    "newPassword": "753123",
}
```

Example Response

```
{
    "success": true,
    "message": "Password reset successful, you can log back into the system.",
    "data": null,
    "timestamp": "2024-11-17T17:27:17.893505158",
    "errors": null
}
```

7.3.7 Get Current User's Profile `GET` `{baseURL}/auth/users/me`

Authenticated users with the role USER can fetch their own information using this endpoint.

No request body or path variable is required.

Header	Type	Mandatory
Authorization	Bearer Token	Yes

Example Response:

```
{
    "status": 200,
    "message": "Current user's profile retrieved successfully.",
    "data": {
        "id": "0384eeb2-12ba-4ca7-907d-55fd5c03891c",
        "keycloakId": "939d5f03-9804-45d8-b287-649664b5752d",
        "username": "johndoe",
        "email": "john@email.com",
        "firstName": "John",
        "lastName": "Doe"
    },
    "timestamp": "2025-01-07T19:52:25.857755524",
    "errors": null
}
```

7.3.8 Get User by ID `GET` `{baseURL}/auth/admin/users/{userId}`

Retrieves a particular user in the system. Accessible only by ADMIN users.

No request body is required.

Path Variable	Type	Mandatory
userId	String	Yes

Header	Type	Mandatory
Authorization	Bearer Token	Yes

Example Response:

```
{
    "status": 200,
    "message": "User with the ID: 90de586d-07e5-49b6-a142-76bf68e42fe8 retrieved successfully.",
    "data": {
        "id": "90de586d-07e5-49b6-a142-76bf68e42fe8",
        "keycloakId": "7d096eec-9be6-492f-be1b-59d9d71d9e93",
        "username": "janedoe",
        "email": "jane@email.com",
        "firstName": "Jane",
        "lastName": "Doe"
    },
    "timestamp": "2025-01-29T20:07:27.949634418",
    "errors": null
}
```

7.3.9 Get All Users `GET` `{baseURL}/auth/admin/users`

Retrieves all users in the system. Accessible only by ADMIN users.

No path variable or header is required.

Header	Type	Mandatory
Authorization	Bearer Token	Yes

Example Response:

```
{
    "status": 200,
    "message": "All users retrieved successfully.",
    "data": [
        {
            "id": "90de586d-07e5-49b6-a142-76bf68e42fe8",
            "keycloakId": "7d096eec-9be6-492f-be1b-59d9d71d9e93",
            "username": "janedoe",
            "email": "jane@email.com",
            "firstName": "Jane",
            "lastName": "Doe"
        },
        {
            "id": "5f6277c8-476b-47c5-8d12-84fbedcb4822",
            "keycloakId": "63e0b928-3f70-4773-8511-6cecea9c2c4e",
            "username": "johndoe",
            "email": "john@email.com",
            "firstName": "John",
            "lastName": "Doe"
        },
        {
            "id": "9b2a3877-910a-42b5-9a6b-b400374829e1",
            "keycloakId": "c9548473-a4d4-4d22-9246-3f032c750b90",
            "username": "admin",
            "email": "admin@email.com",
            "firstName": "Admin",
            "lastName": "Admin"
        },
        ... // all other users
    ],
    "timestamp": "2025-01-29T20:06:43.267648322",
    "errors": null
}
```

7.3.10 Update User Role `PATCH` `{baseURL}/auth/admin/users/role`

Updates the role of a particular user. Accessible only by ADMIN users.

No path variable is required.

Request Body Field	Type	Mandatory
userId	String	Yes

newRole	String	Yes

Header	Type	Mandatory
Authorization	Bearer Token	Yes

Example Request:

```
{
    "userId": "90de586d-07e5-49b6-a142-76bf68e42fe8",
    "newRole": "ADMIN"
}
```

Example Response:

```
{
    "status": 200,
    "message": "Role of the user with ID: 90de586d-07e5-49b6-a142-76bf68e42fe8 changed from USER to ADMIN successfully.",
    "data": {
        user_data
    },
    "timestamp": "2025-01-29T20:08:24.725368929",
    "errors": null
}
```

7.3.11 Update User Access `PATCH` `{baseURL}/auth/admin/users/access`

ADMIN users can ban or unban a user using this endpoint.

No path variable is required.

Request Body Field	Type	Mandatory
userId	String	Yes
isBanned	Boolean	Yes

Header	Type	Mandatory
Authorization	Bearer Token	Yes

Example Request:

```
{
    "userId": "90de586d-07e5-49b6-a142-76bf68e42fe8",
    "isBanned": true
}
```

Example Response:

```
{
    "status": 200,
    "message": "Access of the user with the ID: 90de586d-07e5-49b6-a142-76bf68e42fe8 updated successfully.",
    "data": {
        user_data
    },
    "timestamp": "2025-01-29T20:09:13.625654356",
    "errors": null
}
```

7.3.12 Delete User `DELETE` `{baseURL}/auth/admin/users/{userId}`

Deletes a particular user permanently from the system. Accessible only by ADMIN users.

No request body is required.

Path Variable	Type	Mandatory
userId	String	Yes

Header	Type	Mandatory
Authorization	Bearer Token	Yes

Example Response:

```
{
    "status": 200,
    "message": "User with the ID: 0384eeb2-12ba-4ca7-907d-55fd5c03891c deleted successfully.",
    "data": null,
    "timestamp": "2025-01-07T20:51:23.300920738",
    "errors": null
}
```

7.4 Account Service

7.4.1 Create Account `POST` `{baseURL}/accounts`

Authenticated users can create a new bank account using this endpoint. If `initialBalance` is not provided, the account will be created with zero balance. Users can deposit money later on.

No path variable is required.

Request Body Field	Type	Mandatory
`initialBalance`	`Integer`	`No`

Header	Type	Mandatory
`Authorization`	`Bearer Token`	`Yes`

Example Request:

```
{
    "initialBalance": 5000
}
```

Example Response:

```
{
    "status": 201,
    "message": "Account created successfully.",
    "data": {
        "id": "428bc3c3-55c2-4570-8270-b01a70c0462b",
        "IBAN": "MB236665237261",
        "balance": 5000,
        "isBlocked": false,
        "ownerName": "JOHN DOE",
        "ownerId": "10d51766-970d-4efb-a3ff-f4c08b0b63d6",
        "ownerEmail": "john@email.com"
    },
    "timestamp": "2025-01-31T22:33:23.791207201",
    "errors": null
}
```

7.4.2 Update Account Balance `PUT` `{baseURL}/accounts/balance`

Users can deposit money to their account or withdraw money from their account using this endpoint. If the value of the `isDeposit` field is `true`, this is a deposit action, if `false`, then it is a withdrawal.

No path variable is required.

Request Body Field	Type	Mandatory
`accountId`	`String`	`Yes`
`amount`	`Integer`	`Yes`
`isDeposit`	`Boolean`	`Yes`

Header	Type	Mandatory
`Authorization`	`Bearer Token`	`Yes`

Example Request

```
{
    "accountId": "428bc3c3-55c2-4570-8270-b01a70c0462b",
    "amount": 250,
    "isDeposit": true
}
```

Example Response

```
{
    "status": 200,
    "message": "Account balance updated successfully.",
    "data": {
        "id": "428bc3c3-55c2-4570-8270-b01a70c0462b",
        "IBAN": "MB236665237261",
        "balance": 5250.00,
        "isBlocked": false,
        "ownerName": "JOHN DOE",
        "ownerId": "10d51766-970d-4efb-a3ff-f4c08b0b63d6",
        "ownerEmail": "john@email.com"
    },
    "timestamp": "2025-01-31T22:37:12.591149152",
    "errors": null
}
```

7.4.3 Get Current User's Account by ID `GET` `{baseURL}/accounts/{accountId}`

Users can retrieve the information of one particular account that they owe using this endpoint.

No request body is required.

Path Variable	Type	Mandatory
accountId	String	Yes

Header	Type	Mandatory
Authorization	Bearer Token	Yes

Example Response:

```
{
    "status": 200,
    "message": "Account with the ID: 428bc3c3-55c2-4570-8270-b01a70c0462b retrieved successfully.",
    "data": {
        "id": "428bc3c3-55c2-4570-8270-b01a70c0462b",
        "IBAN": "MB236665237261",
        "balance": 5000.00,
        "isBlocked": false,
        "ownerName": "JOHN DOE",
        "ownerId": "10d51766-970d-4efb-a3ff-f4c08b0b63d6",
        "ownerEmail": "john@email.com"
    },
    "timestamp": "2025-01-31T22:40:15.142589346",
    "errors": null
}
```

7.4.4 Get Current User's All Accounts `GET` `{baseURL}/accounts`

Users can retrieve their own accounts' information using this endpoint.

No request body or path variable is required.

Header	Type	Mandatory
Authorization	Bearer Token	Yes

Example Response:

```
{
    "status": 200,
    "message": "Current users' accounts retrieved successfully.",
    "data": [
        {
            "id": "428bc3c3-55c2-4570-8270-b01a70c0462b",
            "IBAN": "MB236665237261",
            "balance": 5000.00,
            "isBlocked": false,
            "ownerName": "JOHN DOE",
            "ownerId": "10d51766-970d-4efb-a3ff-f4c08b0b63d6",
            "ownerEmail": "john@email.com"
        },
        ... // user's other accounts if there any
    ],
    "timestamp": "2025-01-31T22:41:01.539782599",
    "errors": null
}
```

7.4.5 Delete Own Account `DELETE` `{baseURL}/accounts/{accountId}`

Authenticated users can permanently delete their particular bank account.

No request body is required.

Path Variable	Type	Mandatory
accountId	String	Yes

Header	Type	Mandatory
Authorization	Bearer Token	Yes

Example Response:

```
{
    "status": 200,
    "message": "Current user's account with the ID: 6264906c-7740-4393-a384-e559fb780a58 deleted successfully.",
    "data": null,
    "timestamp": "2024-11-17T17:27:17.893505158",
    "errors": null
}
```

7.4.6 Get All Accounts `GET` `{baseURL}/accounts/admin/accounts`

Retrieves all accounts and can only be utilized by ADMIN users.

No request body or path variable is required.

Header	Type	Mandatory
Authorization	Bearer Token	Yes

Example Response:


```
{
    "status": 200,
    "message": "All accounts retrieved successfully.",
    "data": [
        {
            "id": "3287379f-420b-4349-afe2-09185eac44a7",
            "IBAN": "MB719839468319",
            "balance": 1500.00,
            "isBlocked": false,
            "ownerName": "JOHN DOE",
            "ownerId": "5f6277c8-476b-47c5-8d12-84fbedcb4822",
            "ownerEmail": "john@email.com"
        },
        {
            "id": "080b592a-5afb-4041-8ac9-d4baf06a00b2",
            "IBAN": "MB183211955373",
            "balance": 2500.00,
            "isBlocked": false,
            "ownerName": "JANE DOE",
            "ownerId": "90de586d-07e5-49b6-a142-76bf68e42fe8",
            "ownerEmail": "jane@email.com"
        },
        ... // all other accounts
    ],
    "timestamp": "2025-01-29T20:00:54.396300569",
    "errors": null
}
```


7.4.7 Get Account by ID

`GET` `{baseURL}/accounts/admin/accounts/{accountId}`

Retrieves a particular account. Only ADMIN users can utilize this endpoint.

No request body is required.

Path Variable	Type	Mandatory
accountId	String	Yes

Header	Type	Mandatory
Authorization	Bearer Token	Yes

Example Response:


```
{
    "status": 200,
    "message": "Account with the ID: 3287379f-420b-4349-afe2-09185eac44a7 retrieved successfully.",
    "data": {
        "id": "3287379f-420b-4349-afe2-09185eac44a7",
        "IBAN": "MB719839468319",
        "balance": 1500.00,
        "isBlocked": false,
        "ownerName": "JOHN DOE",
        "ownerId": "5f6277c8-476b-47c5-8d12-84fbedcb4822",
        "ownerEmail": "john@email.com"
    },
    "timestamp": "2025-01-29T20:02:51.185657365",
    "errors": null
}
```


7.4.8 Get Accounts by User ID

`GET` `{baseURL}/accounts/admin/users/{userId}/accounts`

Retrieves a user's accounts. Only ADMIN users can utilize this endpoint.

No request body is required.

Path Variable	Type	Mandatory
userId	String	Yes

Header	Type	Mandatory
Authorization	Bearer Token	Yes

Example Response:


```
{
    "status": 200,
    "message": "Accounts belong to the user with ID: 5f6277c8-476b-47c5-8d12-84fbedcb4822 retrieved successfully.",
    "data": [
```

```
        {
            "id": "3287379f-420b-4349-afe2-09185eac44a7",
            "IBAN": "MB719839468319",
            "balance": 1500.00,
            "isBlocked": false,
            "ownerName": "JOHN DOE",
            "ownerId": "5f6277c8-476b-47c5-8d12-84fbedcb4822",
            "ownerEmail": "john@email.com"
        },
        {
            "id": "1fbd8466-e23c-41a7-98f6-f3b7a04811fb",
            "IBAN": "MB341686764804",
            "balance": 4500.00,
            "isBlocked": false,
            "ownerName": "JOHN DOE",
            "ownerId": "5f6277c8-476b-47c5-8d12-84fbedcb4822",
            "ownerEmail": "john@email.com"
        }
    ],
    "timestamp": "2025-01-29T20:04:24.689199234",
    "errors": null
}
```


7.4.9 Update Account Status `PATCH` `{baseURL}/admin/accounts/status`

Blocks or reactivates a bank account. Only ADMIN users can utilize this endpoint.

No path variable is required.

Request Body Field	Type	Mandatory
accountId	String	Yes
isBlocked	Boolean	Yes

Header	Type	Mandatory
Authorization	Bearer Token	Yes

Example Request:

```
{
    "accountId": "428bc3c3-55c2-4570-8270-b01a70c0462b",
    "isBlocked": true
}
```

Example Response:


```
{
    "status": 200,
    "message": "Status of the account with the ID: 428bc3c3-55c2-4570-8270-b01a70c0462b has been updated",
    "data": {
        "id": "428bc3c3-55c2-4570-8270-b01a70c0462b",
        "IBAN": "MB236665237261",
        "balance": 5000.00,
        "isBlocked": true,
        "ownerName": "JOHN DOE",
        "ownerId": "10d51766-970d-4efb-a3ff-f4c08b0b63d6",
        "ownerEmail": "john@email.com"
    },
    "timestamp": "2025-01-31T22:47:13.762084962",
    "errors": null
}
```


7.4.10 Delete Account `DELETE` `{baseURL}/accounts/admin/accounts/{accountId}`

Deletes a bank account using ADMIN authority.

No request body is required.

Path Variable	Type	Mandatory
accountId	String	Yes

Header	Type	Mandatory
Authorization	Bearer Token	Yes

Example Response:

```
{
    "status": 200,
    "message": "Account with the ID: 1fbd8466-e23c-41a7-98f6-f3b7a04811fb has been deleted",
    "data": null,
    "timestamp": "2025-01-29T20:06:01.592236636",
    "errors": null
}
```

7.5 Transaction Service

7.5.1 Create Transaction `POST` `{baseURL}/transactions`

Users can send money to another account using this endpoint.
Note: Instead of **`receiverAccountId`**, you can also use **`receiverAccountIban`** due to client convenience.

No path variable is required.

Request Body Field	Type	Mandatory
`senderAccountId`	`String`	`Yes`
`receiverAccountId || receiverAccountIban`	`String`	`Yes`
`amount`	`String`	`Yes`
`description`	`String`	`Yes`
Header	**Type**	**Mandatory**
`Authorization`	`Bearer Token`	`Yes`

Example Request:

```
{
    "senderAccountId": "3287379f-420b-4349-afe2-09185eac44a7",
    "receiverAccountIban": "MB183211955373",
    "amount": 250,
    "description": "test transaction description"
}
```

Example Response:

```
{
    "status": 201,
    "message": "Transaction created successfully.",
    "data": {
        "id": "b43131dc-a1c9-4c6f-b90a-1833c3b0eaec",
        "senderAccountId": "080b592a-5afb-4041-8ac9-d4baf06a00b2",
        "receiverAccountId": "080b592a-5afb-4041-8ac9-d4baf06a00b2",
        "amount": 50,
        "description": "test transaction description"
    },
    "timestamp": "2025-01-29T19:33:31.485082461",
    "errors": null
}
```

After successful transaction operation, email addresses associated with both sender and receiver accounts should obtain the following notification email template:

Transaction Notification

Dear User,

A transaction has occurred with the following details:

Transaction ID	b5e672bb-b42d-4556-975a-19fe18f568ac
Sender Name	JOHN DOE
Sender IBAN	MB719839468319
Recipient Name	JANE DOE
Recipient IBAN	MB183211955373
Amount	250 USD
Description	test transaction description
Timestamp	2025-01-29 19:33:31

Thank you,
MicroBank Notification Team

© 2024 MicroBank. All rights reserved.

7.5.2 Get Current User's Transaction by ID `GET` `{baseURL}/transactions/me/{transactionId}`

Users can retrieve their particular transaction information using this endpoint.
No request body is required.

Path Variable	Type	Mandatory
transactionId	String	Yes

Header	Type	Mandatory
Authorization	Bearer Token	Yes

Example Response:

```
{
    "status": 200,
    "message": "Transaction with the ID: fe8c4532-8943-4f81-978a-d4cbbe883fa2 retrieved successfully.",
    "data": {
        "id": "fe8c4532-8943-4f81-978a-d4cbbe883fa2",
        "senderAccountId": "f1f9de3d-3edd-408a-8b6f-6661ca043eab",
        "receiverAccountId": "f1f9de3d-3edd-408a-8b6f-6661ca043eab",
        "amount": 250.0000,
        "description": "test transaction description"
    },
    "timestamp": "2025-01-31T22:52:17.681385723",
    "errors": null
}
```

7.5.3 Get Current User's Transactions by Account ID

`GET` `{baseURL}/transactions/me/accounts/{accountId}`

Users can retrieve their particular transaction information using this endpoint.
No request body is required.

Path Variable	Type	Mandatory
accountId	String	Yes

Header	Type	Mandatory
Authorization	Bearer Token	Yes

Example Response:

```
{
    "status": 200,
    "message": "Transactions associated with the current user's account with the ID: 428bc3c3-55c2-4570-8270-b01a70c0462b
retrieved successfully.",
    "data": [
        {
            "id": "903d7324-b506-4e2f-a5c3-97a70907cd16",
            "senderAccountId": "f1f9de3d-3edd-408a-8b6f-6661ca043eab",
            "receiverAccountId": "f1f9de3d-3edd-408a-8b6f-6661ca043eab",
            "amount": 250.0000,
            "description": "test transaction description"
        },
        ... // all other transactions related to this account
    ],
    "timestamp": "2025-01-31T22:54:23.630342156",
    "errors": null
}
```

7.5.4 Get Current User's All Transactions `GET` `{baseURL}/transactions/me`

Users can retrieve all the transactions they made.
No request body or path variable is required.

Header	Type	Mandatory
Authorization	Bearer Token	Yes

Example Response:

```
{
    "status": 200,
    "message": "Transactions associated with the current user retrieved successfully.",
    "data": [
        {
            "id": "903d7324-b506-4e2f-a5c3-97a70907cd16",
            "senderAccountId": "f1f9de3d-3edd-408a-8b6f-6661ca043eab",
            "receiverAccountId": "f1f9de3d-3edd-408a-8b6f-6661ca043eab",
            "amount": 250.0000,
            "description": "test transaction description"
        },
```

```
        ... // all other transactions related to the current user
    ],
    "timestamp": "2025-01-31T22:53:09.247922388",
    "errors": null
}
```

7.5.5 Get Transaction by ID `GET` `{baseURL}/transactions/admin/transactions/{transactionId}`

ADMIN users can retrieve any particular transaction information.

No request body is required.

Path Variable	Type	Mandatory
transactionId	String	Yes
Header	**Type**	**Mandatory**
Authorization	Bearer Token	Yes

Example Response:

```
{
    "status": 200,
    "message": "Transaction with the ID: 903d7324-b506-4e2f-a5c3-97a70907cd16 retrieved successfully.",
    "data": {
        "id": "903d7324-b506-4e2f-a5c3-97a70907cd16",
        "senderAccountId": "f1f9de3d-3edd-408a-8b6f-6661ca043eab",
        "receiverAccountId": "f1f9de3d-3edd-408a-8b6f-6661ca043eab",
        "amount": 250.0000,
        "description": "test transaction description"
    },
    "timestamp": "2025-01-31T22:58:47.807015896",
    "errors": null
}
```

7.5.6 Get Transactions by Account ID `GET` `{baseURL}/transactions/admin/accounts/{accountId}/transactions`

ADMIN users can retrieve transactions belonging to a particular account.

No request body is required.

Path Variable	Type	Mandatory
accountId	String	Yes
Header	**Type**	**Mandatory**
Authorization	Bearer Token	Yes

Example Response:

```
{
    "status": 200,
    "message": "Transactions associated with the account with the ID: f1f9de3d-3edd-408a-8b6f-6661ca043eab retrieved
successfully.",
    "data": [
        {
            "id": "903d7324-b506-4e2f-a5c3-97a70907cd16",
            "senderAccountId": "f1f9de3d-3edd-408a-8b6f-6661ca043eab",
            "receiverAccountId": "f1f9de3d-3edd-408a-8b6f-6661ca043eab",
            "amount": 250.0000,
            "description": "test transaction description"
        },
        ... // all other transactions related to this account
    ],
    "timestamp": "2025-01-31T22:59:59.252485953",
    "errors": null
}
```

7.5.7 Get Transactions by User ID `GET` `{baseURL}/transactions/admin/users/{userId}/transactions`

ADMIN users can retrieve transactions belonging to a particular user.

No request body is required.

Path Variable	Type	Mandatory
userId	String	Yes
Header	**Type**	**Mandatory**
Authorization	Bearer Token	Yes

Example Response:

```
{
```

```
    "status": 200,
    "message": "Transactions associated with the user with the ID: 10d51766-970d-4efb-a3ff-f4c08b0b63d6 retrieved
successfully.",
    "data": [
        {
            "id": "903d7324-b506-4e2f-a5c3-97a70907cd16",
            "senderAccountId": "f1f9de3d-3edd-408a-8b6f-6661ca043eab",
            "receiverAccountId": "f1f9de3d-3edd-408a-8b6f-6661ca043eab",
            "amount": 250.0000,
            "description": "test transaction description"
        },
        ... // all other transactions associated with this user
    ],
    "timestamp": "2025-02-01T00:00:01.877626847",
    "errors": null
}
```


7.5.8 Get All Transactions `GET` `{baseURL}/admin/transactions`

ADMIN users can retrieve all the transactions that have been made.

No request body or path variable is required.

Header	Type	Mandatory
Authorization	Bearer Token	Yes

Example Response:


```
{
    "status": 200,
    "message": "All transaction documents retrieved successfully.",
    "data": [
        {
            "documentUrl": "http://localhost:9000/documents/TRANSACTION-a260798f-e35c-46ad-b5fd-ba4938bee055.pdf?X-A...",
            "transactionId": "a260798f-e35c-46ad-b5fd-ba4938bee055",
            "senderAccountIban": "MB236665237261",
            "receiverAccountIban": "MB394564793497",
            "senderOwnerName": "JOHN DOE",
            "receiverOwnerName": "AHMET ATAR",
            "amount": 250.00,
            "description": "test transaction description",
            "timestamp": "2025-01-31T22:34:53.392312"
        },
        ... // all other transaction documents
    ],
    "timestamp": "2025-01-31T23:55:33.737587689",
    "errors": null
}
```


7.6 Document Service

7.6.1 Get Transaction Document by ID `POST` `{baseURL}/documents/{documentId}`

Retrieves a particular transaction document, and can be utilized by users who have either USER or ADMIN role.

No request body field is required.

Path Variable	Type	Mandatory
transactionId	String	Yes

Header	Type	Mandatory
Authorization	Bearer Token	Yes

Example Response:


```
{
    "status": 200,
    "message": "Transaction document with the ID: 0d6e3cd9-dc06-4eea-8a7b-f22bc0dc4869 retrieved successfully.",
    "data": {
        "documentUrl": "http://localhost:9000/documents/TRANSACTION-a260798f-e35c-46ad-b5fd-ba4938bee055.pdf?X-Amz-A...",
        "documentName": "TRANSACTION-a260798f-e35c-46ad-b5fd-ba4938bee055.pdf",
        "transactionId": "a260798f-e35c-46ad-b5fd-ba4938bee055",
        "senderAccountIban": "MB236665237261",
        "receiverAccountIban": "MB394564793497",
        "senderOwnerName": "JOHN DOE",
        "receiverOwnerName": "AHMET ATAR",
        "amount": 250.00,
        "description": "test transaction description",
```

```
        "timestamp": "2025-01-31T22:34:53.392312"
    },
    "timestamp": "2025-01-31T23:06:33.173545505",
    "errors": null
}
```


7.6.2 Get Transaction Document by Transaction ID `GET` `{baseURL}/documents/transactions/{transactionId}`

Retrieves a particular transaction's document as well as additional information related to the transaction itself.

No request body is required.

Path Variable	Type	Mandatory
transactionId	String	Yes

Header	Type	Mandatory
Authorization	Bearer Token	Yes

Example Response:


```
{
    "status": 200,
    "message": "Transaction document associated with the transaction with the ID: a260798f-e35c-46ad-b5fd-ba4938bee055
retrieved successfully.",
    "data": {
        "documentUrl": "http://localhost:9000/documents/TRANSACTION-a260798f-e35c-46ad-b5fd-ba4938bee055.pdf?X-Amz-A...",
        "documentName": "TRANSACTION-a260798f-e35c-46ad-b5fd-ba4938bee055.pdf",
        "transactionId": "a260798f-e35c-46ad-b5fd-ba4938bee055",
        "senderAccountIban": "MB236665237261",
        "receiverAccountIban": "MB394564793497",
        "senderOwnerName": "JOHN DOE",
        "receiverOwnerName": "AHMET ATAR",
        "amount": 250.00,
        "description": "test transaction description",
        "timestamp": "2025-01-31T22:34:53.392312"
    },
    "timestamp": "2025-01-31T23:12:57.368773584",
    "errors": null
}
```


7.6.3 Get All Transaction Documents `GET` `{baseURL}/documents/admin/transactions`

ADMIN users can retrieve all transaction documents using this endpoint.

No request body is required.

Path Variable	Type	Mandatory
transactionId	String	Yes

Header	Type	Mandatory
Authorization	Bearer Token	Yes

Example Response:


```
{
    "status": 200,
    "message": "All transaction documents retrieved successfully.",
    "data": [
        {
            "documentUrl": "http://localhost:9000/documents/TRANSACTION-e177bd70-ab63-4c0c-a807-75df822da71b.pdf?X...",
            "documentName": "TRANSACTION-e177bd70-ab63-4c0c-a807-75df822da71b.pdf",
            "transactionId": "e177bd70-ab63-4c0c-a807-75df822da71b",
            "senderAccountIban": "MB719839468319",
            "receiverAccountIban": "MB183211955373",
            "senderOwnerName": "JOHN DOE",
            "receiverOwnerName": "JANE DOE",
            "amount": 50.00,
            "description": "test transaction description",
            "timestamp": "2025-01-29T19:53:23.959053"
        },
        {
            "documentUrl": "http://localhost:9000/documents/TRANSACTION-2ec44f7f-14e7-4d01-9524-6dff0203f91c.pdf?X...",
            "documentName": "TRANSACTION-2ec44f7f-14e7-4d01-9524-6dff0203f91c.pdf",
            "transactionId": "2ec44f7f-14e7-4d01-9524-6dff0203f91c",
            "senderAccountIban": "MB183211955373",
            "receiverAccountIban": "MB719839468319",
            "senderOwnerName": "JANE DOE",
            "receiverOwnerName": "JOHN DOE",
            "amount": 120.00,
            "description": "test transaction description 2",
            "timestamp": "2025-01-29T20:12:56.437774"
        },
```

```
        ... // all other transaction documents
    ],
    "timestamp": "2025-01-29T20:17:31.23600947",
    "errors": null
}
```

7.7 Notification Service

The Notification Service is a critical component of the MicroBank project, designed to facilitate event-driven communication. It functions as a message consumer, processing messages from predefined queues to notify users about important events. This microservice does not expose any RESTful endpoints for direct client interaction. Instead, it continuously listens to message queues and triggers email notifications accordingly.

As part of the event-driven communication model, MicroBank utilizes three distinct message queues:

- `activation-queue`
- `password-recovery-queue`
- `transaction-queue`

The Notification Service constantly listens to these queues separately and processes the received messages to send the necessary email notifications. For a detailed breakdown of this service's responsibilities, refer to sections **7.3.1**, **7.3.5**, and **7.5.1**.

- The Activation Queue is triggered after a user successfully registers an account. It processes the temporary user data and sends an activation email containing the activation code.
- The Password Recovery Queue is triggered when a user requests a password reset via the "Forgot Password" endpoint. Similar to the activation queue, it processes the request and sends an email containing a password recovery code.
- The Transaction Queue is triggered after a successful financial transaction. This queue handles the transaction event, generates the transaction receipt document, and sends transaction details via email to both the sender and the recipient.

This microservice ensures that all critical user actions are accompanied by timely and automated notifications, enhancing the overall banking experience.