PFP FFA Platform technical & functionals specifications

1. Introduction

2. Background

3. Goal

- Develop a complete web application (frontend, back office, and backend) to publish FFA's projects, allowing people to apply and compile published projects.

4. Functionalities

4.1 Administrators (Back Office)

1. Do everything Interveners can do
2. Manage interveners

4.2 Interveners (Back Office)

1. Register and specify their decentralized cooperation department.
2. Indicate their affiliated entity (embassies and countries, departments, regions, or cities).
3. Securely and confidentially submit projects.
4. Receive alerts for project responses.
5. Access a personal message inbox.
6. View all projects on the platform.

4.3   Users (Frontend)

1. Register, log in, and log out.

2. View all projects on the platform without logging in.

3. Apply for projects by submitting the required documents.

4. Receive alerts for responses from the interveners.

5. Access a personal message inbox.

4.4   Core Features

1. User authentication for all platform functionalities.

2. Access control management based on user roles.

3. Responsive web application accessible via smartphones, tablets, and computers.

4. Strong security measures for all communications.

4.5   Non-functional Requirements

1. Performance:

   - The system should handle concurrent users effectively.

2. Usability:

   - The interface should be intuitive and easy to navigate.

3. Reliability:

   - The system should have 99.9% availability.
   - It should have robust error-handling mechanisms.

4. Security:

   - Data should be strongly encrypted during transmission and storage.
   - Regular security audits and updates should be conducted.

5. Scalability:

   - The system should be scalable to accommodate future growth.

6. Maintainability:

   - Code should be well-documented and follow best practices.

5. Plan

5.1   Website Development

5.1.1   Website Structure

1. Frontend: Interacts with users and captures input.

2. Backend (REST API): Processes input, handles business logic, and communicates with the database.

3. Database: Stores and retrieves data as needed.

4. Back Office: Manages administrative tasks and ensures system integrity.

5.1.2 Tech Stack

1. Frontend and Back Office:

   - HTML, CSS, JavaScript
   - Vue.js
   - Primefaces for UI components

2. Backend:

   - Spring Boot as the application framework
   - REST API for communication between (frontend, back-office) and backend
   - Apache Shiro, Spring Authorization Server, Spring Security for security
   - FastJson for JSON processing
   - Apache Commons Lang and IO for utility functions
   - Hutool for Java utilities
   - Javax Validation for validation
   - Protobuf for protocol buffers

3. Database:

   - PostgreSQL

4. Database Connection Tool:

   Hibernate or Mybatis-Plus or ???

6. Security, Privacy and Risk Management

6.1 Security Vulnerabilities

Risk Description: Unauthorized access, data breaches, and hacking could lead to the disclosure of sensitive information.
Solution: Implement strong encryption technologies (such as SSL/TLS) to protect data transmission. Use multi-factor authentication (MFA) to enhance access control security. Conduct regular security audits and penetration tests to identify and fix vulnerabilities.

6.2 Data Loss

Risk Description: Data loss due to system failures or human error could severely impact the business. **Solution**: Implement a regular data backup strategy to ensure data can be restored in case of failure. Use redundant storage and disaster recovery plans to quickly recover from data loss incidents.

6.3 Privacy Protection

Risk Description: High concurrent access could lead to slow system response or crashes.
Solution: Conduct load testing to identify and resolve performance bottlenecks. Use caching mechanisms and load balancing technologies to improve system handling capacity.

6.4 Security Vulnerabilities

- **Data Minimization**: Collect, store, and process only the minimum data required for project operation.

- **Anonymization**: Anonymize user data as soon as possible to prevent the disclosure of personal identity information.

- **User Control**: Provide tools for users to manage their personal data, including data access, correction, and deletion requests.

7. FFA platform Database

This database diagram can be improved