**Software Requirements Specification (SRS) for User Auth**

Revision History

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Revision** | **Date** | **JIRA Ticket Number** | **Change Description** | **Author** | **Reviewed By** | **Approved By** |
| 1.0 | 18-09-2023 | - | Initial version | Abde Ali | - | - |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |

## **1. Introduction**

### **1.1 Purpose**

The purpose of this document is to specify the functional and non-functional requirements for the development of the SignUp\_SignIn\_API with authentication methods. This API will enable users to sign up, sign in, reset their password, verify email addresses, and log out using various authentication providers, including Google, Hubspot, Facebook, Instagram, LinkedIn, and Twitter.

### **1.2 Scope**

The SignUp\_SignIn\_API will encompass the following features:

* User registration (SignUp)
* User login (SignIn)
* Password reset (ResetPassword)
* Email verification (VerifyEmail)
* User logout (LogOut)
* Integration with multiple authentication providers (Google, Hubspot, Facebook, Instagram, LinkedIn, Twitter)

## **2. User Authentication**

### **2.1 Functional Requirements**

#### **SignUp**

* User registration with required information (e.g., email, username, password).
* Validation of user input data.
* Generation of a unique user identifier.
* Storage of user data in the database.
* Sending a verification email to the user.

#### **SignIn**

* Authentication of users with valid credentials.
* Handling authentication via different providers (e.g., email/password, social media).
* Token generation and management for authenticated sessions.

#### **ResetPassword**

* User-initiated password reset process.
* Validation of the reset request.
* Sending a password reset email with a unique token.
* Updating the user's password after token verification.

#### **VerifyEmail**

* Verification of user email addresses via a confirmation link.
* Activation of user accounts upon email verification.
* Handling email verification for different registration methods.

#### **LogOut**

* Terminating user sessions and revoking authentication tokens.
* Ensuring that the user is logged out securely.

### **2.2 Non-Functional Requirements**

* Security measures for protecting user data and authentication tokens.
* Error handling and logging for debugging and monitoring.

## **3. Authentication Providers Integration**

### **3.1 Functional Requirements**

* Integration with Google authentication.
* Integration with Hubspot authentication.
* Integration with Facebook authentication.
* Integration with Instagram authentication.
* Integration with LinkedIn authentication.
* Integration with Twitter authentication.
* Handling of provider-specific authentication flows and responses.

### **3.2 Non-Functional Requirements**

* Compliance with authentication provider APIs and security standards.
* Flexibility to add support for additional authentication providers in the future.
* Usability and user experience in the authentication process with various providers.

## **5. Conclusion**

This Software Requirements Specification outlines the functional and non-functional requirements for developing the SignUp\_SignIn\_API with authentication methods, including integration with various authentication providers. The API should provide secure and user-friendly authentication and user management functionalities.

Please note that this is a high-level outline, and each section should be expanded with more specific details, use cases, and acceptance criteria to guide the development of the API effectively.