# *Software Requirements Specification (SRS)*

**Project: SkillSwap Mobile Application**

**Document: Login Module SRS Document**

**Version: 1.0**

**Date: September 25, 2025**

## 1. Introduction

### 1.1 Purpose

This document provides a comprehensive and detailed specification of the functional and non-functional requirements for the user login module of the SkillSwap mobile application. Its purpose is to serve as a foundational guide for the development, quality assurance, and project management teams, ensuring a clear and shared understanding of all module requirements.

### 1.2 Scope

This SRS is focused exclusively on the user authentication and login process. It specifies the required user interfaces, authentication methods, user data handling, and the navigation flow from the login screen to the main application view. It does not cover the back-end system architecture, user registration, or password recovery functionalities.

### 1.3 Definitions, Acronyms, and Abbreviations

***SRS: Software Requirements Specification***

UI: User Interface

OTP: One-Time Password

FR: Functional Requirement

NFR: Non-Functional Requirement

## 2. Overall Description

### 2.1 Product Perspective

The login module is a critical, self-contained component of the SkillSwap mobile application. It is the primary point of entry for all authenticated users and must provide a secure and intuitive experience consistent with the overall application design.

### 2.2 Product Functions

The login module's primary functions are to:

Validate user identity through various authentication methods.

Manage a seamless and secure entry point into the application.

Provide a clear and aesthetically pleasing user interface.

### 2.3 User Characteristics

The target audience consists of mobile users with varying technical proficiencies. The login process must be simple enough for novice users while providing the security and flexibility expected by more experienced users.

## 3. Specific Requirements

### 3.1 Functional Requirements (FR)

FR1: Email/Password Authentication

***FR1.1:*** The system shall display a form with two input fields labeled "Email Address" and "Password."

***FR1.2:*** The system shall validate the user's input against stored credentials upon

pressing the "Log In" button.

***FR1.3:*** Upon successful authentication, the system shall transition the user to

the HomeScreen

***FR1.4:*** If authentication fails, the system shall display an error message informing the user of invalid credentials.

***FR2: Passwordless Authentication (OTP/Magic Link)***

***FR2.1: The system shall provide an option to switch to a passwordless login flow.***

FR2.2: When this flow is selected, the system shall provide a single input field for the user's email address.

FR2.3: Upon pressing the "Get OTP / Magic Link" button, the system shall send an email containing a secure, single-use login token to the provided address.

FR2.4: The system shall provide a clear confirmation message to the user that the email has been sent.

FR3: Third-Party Authentication (Google)

FR3.1: The system shall include a button clearly labeled "Sign In with Google."

FR3.2: Tapping this button shall initiate the Google Sign-In authentication flow.

FR3.3: Upon successful authentication via Google, the system shall automatically create or link a user account and transition the user to the HomeScreen.

FR4: Navigation

FR4.1: A back button or similar navigation control shall be present on the login screen.

FR4.2: This control shall navigate the user back to the previous screen in the navigation stack.

### 3.2 Non-Functional Requirements (NFR)

NFR1: Performance: The login process, from button press to screen transition, shall be completed within 2 seconds under normal network conditions.

NFR2: Usability: The UI shall be intuitive, with clear labels and a logical flow. Input fields shall provide visual feedback when focused.

NFR3: Security: All data transmitted for authentication shall be encrypted. The password input field shall obscure characters to protect sensitive information.

NFR4: Compatibility: The user interface shall be responsive and fully functional on all major mobile operating systems (iOS and Android) and screen sizes. The UI shall handle on-screen keyboard visibility without obstructing critical content.

NFR5: Maintainability: The code for the login module shall be organized into reusable components and functions, adhere to a consistent naming convention, and include inline documentation to explain complex logic.

### 4. User Interface Requirements

UI1: Visual Design: The screen shall use a two-color linear gradient background. The primary color shall be #4A90E2 and the secondary accent color shall be #FF3366.

UI2: Animations: The "Welcome to SkillSwap" text shall animate with a continuous color transition. The main content area shall fade in smoothly upon screen load.

UI3: Interactive Elements: Buttons shall have a modern, elevated design. The Google login button shall include a recognizable Google icon.