

# Project Phoenix: User Authentication Specification v1.0

**Company Logo** [Insert your company logo here]

**Document Version:** 1.0

**Date:** April 18, 2025

**Author:** [Your Name]

## Introduction

This document outlines the requirements for the initial user authentication module for Project Phoenix. It covers user registration, login via email/password, and basic password reset functionality.

## Requirements

### 1. User Registration

- Users must be able to register using a unique email address and a password meeting complexity requirements (min 8 chars, 1 uppercase, 1 number).
- The system must validate email uniqueness before completing registration.
- Upon successful registration, users should receive a confirmation email.

### 2. User Login

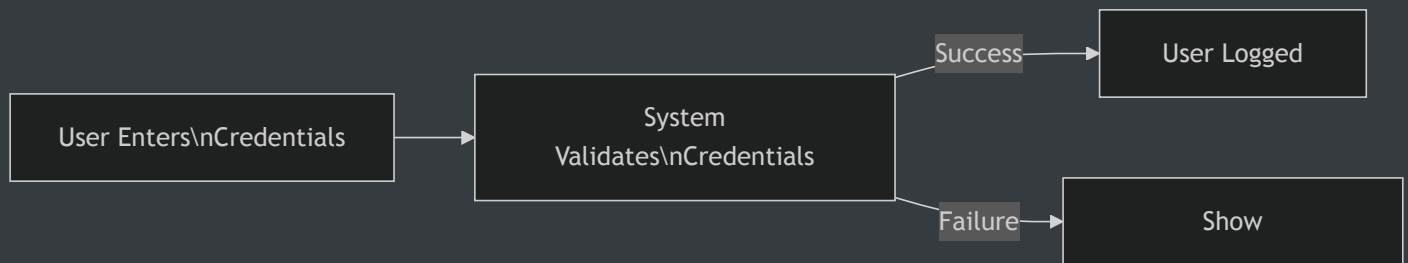
- Registered users must be able to log in using their email and password.
- Failed login attempts should display appropriate error messages.
- The system should implement rate limiting for failed login attempts.

### 3. Password Reset

- A 'Forgot Password' flow must allow users to reset their password via an email link.
- Password reset links should expire after 24 hours.
- Users must confirm their new password by typing it twice.

## Authentication Flow

Figure 1: Basic Login Flow



## Out of Scope

The following items are explicitly out of scope for v1.0:

- OAuth
- Two-factor authentication (2FA)
- Social media logins

## Next Steps

Implementation will begin once this specification is approved by all stakeholders.

---

**Document Approvals:**

Role	Name	Date	Signature
Product Manager			
Engineering Lead			
Security Lead			