# Business Requirements Document

# User Registration and Authentication

## Document Control

|  |  |
| --- | --- |
| Item | Description |
| Document Title | User Registration and Authentication - Business Requirements Document |
| Document Version | 1.0 |
| Document Status | Draft |
| Document Owner | [Document Owner] |
| Last Updated | March 20, 2025 |

## 1. Introduction

### 1.1 Purpose

This document outlines the business requirements for the User Registration and Authentication component of the Emtelaak Platform, a real estate investment platform enabling fractional property ownership. This component is responsible for user onboarding, identity verification, authentication, and user profile management.

### 1.2 Scope

The User Registration and Authentication system will handle the following processes:

* User registration
* Identity verification (KYC/AML)
* Investor accreditation
* Authentication and authorization
* User profile management
* Role-based access control

### 1.3 References

* Project Charter (project-charter.docx)
* Development Approach and Tech Stack (development-approach.docx)
* Feature Comparison with Similar Platforms (emtelaak-feature-comparison.docx)
* User Registration Flow (User Registration flow.pdf)

## 2. Stakeholders

### 2.1 Business Stakeholders

* Executive Sponsors
* Product Owner
* Legal & Compliance Team
* Marketing Team

### 2.2 Technical Stakeholders

* Project Manager
* Technical Architect
* Development Team
* QA Team
* Security Team

### 2.3 End Users

* Investors (Individuals seeking to invest in properties)
* Issuers (Property owners/managers looking to list properties)
* Platform Administrators

## 3. Business Objectives

### 3.1 Primary Objectives

1. Create a secure and compliant user registration system that meets all regulatory requirements
2. Implement robust KYC/AML verification processes
3. Establish investor accreditation verification
4. Provide an intuitive, frictionless onboarding experience
5. Support different user types with role-based permissions
6. Ensure data privacy and protection compliance

### 3.2 Success Criteria

1. 95% or higher user registration completion rate
2. KYC verification process completed in under 24 hours
3. 100% compliance with relevant financial regulations
4. User profile data secured with industry-standard encryption
5. Support for at least 10,000 concurrent users with optimal performance

## 4. Business Requirements

### 4.1 User Registration Requirements

#### 4.1.1 General Registration

1. **User Registration Flow**
   * System shall provide a step-by-step registration process
   * Users shall provide basic information: name, email, password, phone number
   * Email verification required before account activation
   * Phone verification via SMS for added security
   * Terms of service and privacy policy acceptance required
2. **User Types**
   * System shall support registration for different user types:
     + Individual Investors
     + Institutional Investors
     + Property Issuers (Owners/Managers)
     + Platform Administrators
3. **Profile Information**
   * Users shall provide and manage the following information:
     + Personal details (name, contact information)
     + Address information
     + Communication preferences
     + Notification settings
     + Document uploads (ID, proof of address, etc.)

#### 4.1.2 KYC/AML Verification

1. **Identity Verification**
   * Integration with third-party KYC service provider
   * Document verification (government-issued ID, passport)
   * Facial recognition verification option
   * Address verification
2. **Verification Status**
   * Track verification status (Pending, In Progress, Verified, Rejected)
   * Notification to users about verification status
   * Option to resubmit verification if rejected
3. **Ongoing Monitoring**
   * Periodic re-verification based on risk assessment
   * Transaction monitoring for suspicious activities
   * Automated flagging of unusual account activities

#### 4.1.3 Investor Accreditation

1. **Accreditation Verification**
   * Financial information collection for accreditation assessment
   * Document upload for income/net worth verification
   * Third-party verification integration
   * Accreditation status tracking and renewal
2. **Investor Classification**
   * Classification based on jurisdiction requirements
   * Support for different investor types (Accredited, Non-Accredited, Qualified)
   * Investment limits based on investor classification

### 4.2 Authentication Requirements

#### 4.2.1 Login and Authentication

1. **Authentication Methods**
   * Email and password authentication
   * Multi-factor authentication (MFA)
   * Biometric authentication for mobile app
   * Single sign-on (SSO) options
2. **Session Management**
   * Secure session handling
   * Configurable session timeout
   * Multiple device management
   * Active session tracking
3. **Password Management**
   * Strong password requirements
   * Password reset functionality
   * Password change history
   * Account lockout after failed attempts

#### 4.2.2 Authorization and Access Control

1. **Role-based Access Control**
   * Role definition for different user types
   * Permission management
   * Role assignment and modification
   * Access restrictions based on user role
2. **Permission Sets**
   * Granular permission sets for system functions
   * Custom permission configurations
   * Permission inheritance and overrides

### 4.3 User Profile Management

#### 4.3.1 Profile Management

1. **Profile Updates**
   * Self-service profile updates
   * Verification of critical information changes
   * Profile completion tracking
   * Profile picture management
2. **Settings Management**
   * Privacy settings
   * Notification preferences
   * Language preferences
   * Display preferences

#### 4.3.2 Account Management

1. **Account Status**
   * Active/Inactive status
   * Account suspension
   * Account deletion/deactivation
   * Account reinstatement
2. **Logs and History**
   * Login history
   * Activity logging
   * Security alerts
   * Changes to sensitive information

## 5. Integration Requirements

### 5.1 External System Integrations

1. **KYC/AML Service Providers**
   * Integration with identity verification services
   * Document verification API
2. **Communication Services**
   * Email service integration
   * SMS notification service
   * Push notification service

### 5.2 Internal System Integrations

1. **Wallet System**
   * User account linking to wallet
   * Authorization for financial transactions
2. **Investment System**
   * User verification status checking
   * Investor classification for investment eligibility
3. **Notification System**
   * User communication preferences
   * Alert configuration

## 6. Non-functional Requirements

### 6.1 Security Requirements

1. **Data Protection**
   * Data encryption at rest and in transit
   * Secure storage of verification documents
   * Data access audit trails
2. **Authentication Security**
   * HTTPS/TLS for all communications
   * OAuth 2.0 and OpenID Connect protocols
   * JWT token-based authentication
   * Protection against common vulnerabilities (OWASP Top 10)

### 6.2 Performance Requirements

1. **Response Times**
   * Registration process completion < 5 minutes
   * Authentication < 2 seconds
   * Profile updates < 3 seconds
2. **Scalability**
   * Support for 10,000+ concurrent users
   * Support for 1,000+ simultaneous registrations
   * Elastic scaling during peak periods

### 6.3 Availability Requirements

1. **System Uptime**
   * 99.9% uptime for authentication services
   * 24/7 availability with planned maintenance windows
   * Redundancy for critical components

### 6.4 Compliance Requirements

1. **Regulatory Compliance**
   * Compliance with applicable financial regulations
   * Record keeping requirements
   * Audit trail for compliance verification

## 7. User Experience Requirements

### 7.1 Registration Experience

1. **User-friendly Interface**
   * Intuitive registration flow
   * Clear guidance and instructions
   * Progress indicators
   * Mobile-responsive design
2. **Error Handling**
   * Clear error messages
   * Guidance for correction
   * Field validation

### 7.2 Authentication Experience

1. **Login Experience**
   * Remember me functionality
   * Quick access options
   * Biometric authentication for mobile
   * Streamlined MFA process
2. **Account Recovery**
   * Simple password reset process
   * Alternative verification methods
   * Account recovery options

## 8. Reporting Requirements

### 8.1 User Analytics

1. **Registration Analytics**
   * Conversion rates
   * Abandonment points
   * Time to complete registration
   * Verification success rates
2. **User Activity Reporting**
   * Login frequency
   * Failed login attempts
   * Account usage patterns
   * Inactive account identification

### 8.2 Compliance Reporting

1. **KYC/AML Reporting**
   * Verification status reports
   * Rejection reasons
   * Verification time metrics
   * Suspicious activity reports
2. **Audit Reporting**
   * User activity audit logs
   * Admin activity audit logs
   * System access reports
   * Changes to sensitive information

## 9. Constraints and Assumptions

### 9.1 Constraints

1. Must comply with all relevant financial regulations and securities laws
2. Must integrate with specified third-party KYC/AML providers
3. Must be compatible with both web and mobile interfaces
4. Must adhere to organizational security standards

### 9.2 Assumptions

1. Third-party KYC/AML service providers will be available and responsive
2. Regulatory framework will remain stable during development
3. Users will have access to required verification documents
4. Mobile devices will support biometric authentication

## 10. Appendices

### 10.1 Glossary

* **KYC**: Know Your Customer
* **AML**: Anti-Money Laundering
* **MFA**: Multi-Factor Authentication
* **SSO**: Single Sign-On
* **JWT**: JSON Web Token

### 10.2 Related Documents

* User Registration Flow Diagram
* Registration UI Mockups
* API Specifications
* Data Schema
* Security Standards Document