Software Requirements Specification

User Registration and Authentication

Document Control

Item	Description
Document Title	User Registration and Authentication - Software Requirements Specification
Document Version	1.0
Document Status	Draft
Document Owner	[Document Owner]
Last Updated	March 27, 2025
Related Documents	Business Requirements Document v1.0 (March 20, 2025)

1. Introduction

1.1 Purpose

This Software Requirements Specification (SRS) document details the functional and non-functional requirements for the User Registration and Authentication component of the Emtelaak Platform. It serves as a comprehensive guide for the development team, QA team, and other technical stakeholders to implement a secure and compliant user onboarding experience.

1.2 Scope

The User Registration and Authentication system encompasses:

- User registration and account creation
- Identity verification (KYC/AML)
- Investor accreditation verification
- Authentication mechanisms and protocols
- Authorization and role-based access control
- User profile management
- Security and compliance controls

1.3 Definitions, Acronyms, and Abbreviations

Term	Definition
API	Application Programming Interface
CCPA	California Consumer Privacy Act
GDPR	General Data Protection Regulation
JWT	JSON Web Token
KYC/AML	Know Your Customer/Anti-Money Laundering
MFA	Multi-Factor Authentication
OAuth	Open Authorization
OTP	One-Time Password
PEP	Politically Exposed Person
PII	Personally Identifiable Information
RBAC	Role-Based Access Control
REST	Representational State Transfer
SSO	Single Sign-On
TLS	Transport Layer Security
UI	User Interface
UX	User Experience

1.4 References

- Emtelaak 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)
- User Registration and Authentication BRD v1.0 (user-registration-brd.docx)

1.5 Overview

This document is organized into the following sections:

- Introduction: Provides context and background information
- Overall Description: Describes product perspective and functionality
- System Features: Details specific features and functional requirements
- External Interface Requirements: Specifies user, hardware, software, and communication interfaces
- Non-Functional Requirements: Outlines performance, security, usability, and other quality attributes

- Other Requirements: Covers additional technical and business requirements

2. Overall Description

2.1 Product Perspective

The User Registration and Authentication component is a foundational subsystem of the Emtelaak Platform. It interfaces with several other platform components:

1. **Wallet System**: For linking verified user accounts to financial wallets
2. **Investment System**: For enforcing investment eligibility based on user verification status
3. **Property Listing System**: For controlling access to property data based on user roles
4. **Secondary Market System**: For enabling transaction authorization
5. **Notification System**: For sending verification and authentication alerts

The system also integrates with third-party services for KYC/AML verification, communication channels (email, SMS), and potentially SSO providers.

2.2 Product Functions

At a high level, the system will provide the following functions:

1. User registration with step-by-step guided flow
2. Identity verification and KYC/AML compliance
3. Investor accreditation verification
4. Secure authentication with multi-factor capabilities
5. Role-based access control for different user types
6. User profile management and settings configuration
7. Account status management (active, suspended, deleted)
8. Audit logging and compliance reporting

2.3 User Classes and Characteristics

The system supports multiple user classes, each with specific characteristics:

1. **Individual Investors**
   - Require KYC verification
   - May need accreditation verification
   - Focused on investment activities

- Varying levels of technical expertise

2. **Institutional Investors**
   - Require enhanced due diligence
   - Complex ownership structure verification
   - Often have specific compliance requirements
   - May have multiple authorized users
3. **Property Issuers (Owners/Managers)**
   - Require enhanced KYC verification
   - Need access to property listing features
   - May represent organizations or companies
   - Focused on property management functionality
4. **Platform Administrators**
   - Internal users with elevated privileges
   - Access to system administration functions
   - Higher security requirements
   - Technical expertise expected

2.4 Operating Environment

The User Registration and Authentication system will operate in the following environment:

- **Server Environment**: Microsoft Azure cloud infrastructure
- **Backend Framework**: ASP.NET Core 8
- **Database**: SQL Server for user data, Azure Blob Storage for documents
- **Authentication Server**: IdentityServer4
- **Web Client**: Modern browsers (Chrome, Firefox, Safari, Edge)
- **Mobile Client**: iOS and Android devices via Flutter app

2.5 Design and Implementation Constraints

1. **Regulatory Compliance**: Must adhere to financial regulations, securities laws, and data protection requirements (GDPR, CCPA)
2. **Third-Party Services**: Limited by the capabilities and APIs of selected KYC/AML service providers
3. **Security Standards**: Must implement industry best practices and organizational security standards
4. **Cross-Platform Compatibility**: Must function consistently across web and mobile interfaces

5. **Integration Requirements**: Must integrate with existing platform components and third-party services
6. **Performance Constraints**: Must handle specified user load and meet response time requirements

2.6 User Documentation

The system will include the following user documentation:

1. User registration guide
2. KYC/AML verification instructions
3. Account management tutorial
4. Security best practices guide
5. Mobile app authentication guide
6. FAQ for common issues

2.7 Assumptions and Dependencies

1. **Third-Party Services**: Depends on the availability and performance of KYC/AML service providers
2. **Regulatory Framework**: Assumes relative stability in regulatory requirements during development
3. **Technical Infrastructure**: Depends on Azure cloud services and related infrastructure
4. **Client Devices**: Assumes users have devices that support required security features (e.g., biometrics)
5. **Cross-System Integration**: Depends on APIs from other platform components being available as specified

3. System Features

3.1 User Registration

3.1.1 Description

The system shall provide a comprehensive user registration process that collects necessary information while minimizing friction. Registration will be step-based, allowing users to save progress and continue later.

3.1.2 Functional Requirements

1. **REG-1**: The system shall provide a multi-step registration wizard with progress indicators
   - **REG-1.1**: Users shall be able to save progress and continue registration later
   - **REG-1.2**: The system shall validate each step before allowing progression

- **REG-1.3**: The system shall support registration across web and mobile platforms with consistent experience

2. **REG-2**: The system shall collect the following basic information during initial registration:
   - **REG-2.1**: Email address (required, must be unique in system)
   - **REG-2.2**: Password (required, must meet complexity requirements)
   - **REG-2.3**: Full name (required)
   - **REG-2.4**: Phone number (required)
   - **REG-2.5**: User type selection (required)
3. **REG-3**: The system shall verify user email through a confirmation link
   - **REG-3.1**: Email verification link shall expire after 24 hours
   - **REG-3.2**: Users shall be able to request a new verification email
   - **REG-3.3**: Account shall remain in unverified state until email is confirmed
4. **REG-4**: The system shall verify user phone number through SMS OTP
   - **REG-4.1**: SMS code shall expire after 10 minutes
   - **REG-4.2**: Users shall be able to request a new verification code (maximum 3 attempts within 24 hours)
   - **REG-4.3**: System shall provide alternative verification method if SMS delivery fails
5. **REG-5**: The system shall require acceptance of terms of service and privacy policy
   - **REG-5.1**: Terms acceptance shall be recorded with timestamp and IP address
   - **REG-5.2**: Users must explicitly check acceptance box (not pre-checked)
   - **REG-5.3**: Terms updates shall require re-acceptance upon next login
6. **REG-6**: The system shall collect additional information based on user type:
   - **REG-6.1**: Individual investors: date of birth, residential address, nationality, employment information
   - **REG-6.2**: Institutional investors: organization name, registration number, business address, authorized representatives
   - **REG-6.3**: Property issuers: organization details, business license, contact information
7. **REG-7**: The system shall allow document uploads for verification purposes
   - **REG-7.1**: Supported document types shall include JPG, PNG, and PDF formats
   - **REG-7.2**: Maximum file size shall be 10MB per document
   - **REG-7.3**: Uploaded documents shall be encrypted at rest
   - **REG-7.4**: Required documents shall be clearly indicated based on user type

8. **REG-8**: The system shall create a user account with unique identifier upon successful registration
    - **REG-8.1**: Account shall be created with appropriate initial status (unverified)
    - **REG-8.2**: Default user role shall be assigned based on user type
    - **REG-8.3**: Welcome email shall be sent upon account creation

3.2 KYC/AML Verification

3.2.1 Description

The system shall implement robust KYC/AML verification processes to ensure regulatory compliance and prevent fraudulent activities. This will involve identity verification, document validation, and ongoing monitoring.

3.2.2 Functional Requirements

1. **KYC-1**: The system shall integrate with third-party KYC/AML service providers
    - **KYC-1.1**: Integration shall support RESTful API communication
    - **KYC-1.2**: Fallback mechanism shall be implemented for service disruptions
    - **KYC-1.3**: Integration shall support webhooks for asynchronous verification updates
2. **KYC-2**: The system shall support document verification for identity confirmation
    - **KYC-2.1**: Acceptable ID documents shall include passport, national ID card, and driver's license
    - **KYC-2.2**: Document authenticity verification shall check for tampering and validity
    - **KYC-2.3**: System shall extract and validate personal information from documents
    - **KYC-2.4**: System shall compare extracted information with user-provided information
3. **KYC-3**: The system shall support facial recognition verification
    - **KYC-3.1**: Selfie photo shall be compared with ID document photo
    - **KYC-3.2**: Liveness detection shall be implemented to prevent spoofing
    - **KYC-3.3**: Alternative verification method shall be available if facial recognition fails
4. **KYC-4**: The system shall verify user address through appropriate documentation
    - **KYC-4.1**: Acceptable proof of address shall include utility bills, bank statements, and government letters
    - **KYC-4.2**: Documents must be dated within the last 3 months
    - **KYC-4.3**: Address extraction and validation shall be performed automatically where possible
5. **KYC-5**: The system shall perform watchlist screening
    - **KYC-5.1**: Screening shall include sanctions lists, PEP lists, and adverse media

- **KYC-5.2**: Screening shall be performed at registration and periodically thereafter
- **KYC-5.3**: Matches shall be flagged for manual review with risk scoring

6. **KYC-6**: The system shall track verification status with appropriate states
   - **KYC-6.1**: Status states shall include Pending, In Progress, Verified, Rejected, and Additional Information Required
   - **KYC-6.2**: Status changes shall trigger appropriate notifications
   - **KYC-6.3**: Status history shall be maintained for audit purposes
7. **KYC-7**: The system shall support reverification and periodic reviews
   - **KYC-7.1**: Automatic reverification shall be triggered based on risk level (6-24 months)
   - **KYC-7.2**: Significant profile changes shall trigger partial reverification
   - **KYC-7.3**: Users shall be notified before reverification is required
8. **KYC-8**: The system shall implement risk-based verification levels
   - **KYC-8.1**: Risk assessment shall consider user type, location, investment amount, and activity patterns
   - **KYC-8.2**: Enhanced due diligence shall be applied to high-risk cases
   - **KYC-8.3**: Verification requirements shall adjust based on risk level

3.3 Investor Accreditation

3.3.1 Description

The system shall verify investor accreditation status to comply with securities regulations and enable appropriate investment access based on investor classification.

3.3.2 Functional Requirements

1. **ACC-1**: The system shall collect financial information for accreditation assessment
   - **ACC-1.1**: Income information collection with documentation options
   - **ACC-1.2**: Net worth declaration with supporting documentation options
   - **ACC-1.3**: Professional certifications or qualifications relevant to accreditation
   - **ACC-1.4**: Investment experience and history (optional)
2. **ACC-2**: The system shall support document upload for accreditation verification
   - **ACC-2.1**: Acceptable documents shall include tax returns, bank statements, investment accounts, and certification letters
   - **ACC-2.2**: Document validation shall check completeness and relevance

- **ACC-2.3**: Document metadata shall be recorded (upload date, document type, verification status)

3. **ACC-3**: The system shall integrate with third-party accreditation verification services
   - **ACC-3.1**: API integration with verification providers
   - **ACC-3.2**: Support for manual review and verification by compliance team
   - **ACC-3.3**: Verification request tracking and status updates
4. **ACC-4**: The system shall classify investors according to regulatory categories
   - **ACC-4.1**: Classification shall include Accredited, Non-Accredited, Qualified, etc. as per jurisdiction
   - **ACC-4.2**: Classification rules shall be configurable per jurisdiction
   - **ACC-4.3**: Multiple classifications shall be supported for cross-border investors
5. **ACC-5**: The system shall enforce investment limits based on investor classification
   - **ACC-5.1**: Investment limits shall be configurable per offering type and jurisdiction
   - **ACC-5.2**: Pre-investment checks shall verify eligibility based on classification
   - **ACC-5.3**: Override capability shall be available to administrators with appropriate approval workflow
6. **ACC-6**: The system shall track accreditation expiration and renewal
   - **ACC-6.1**: Accreditation shall expire after configurable period (default 12 months)
   - **ACC-6.2**: Renewal notifications shall be sent 30, 15, and 5 days before expiration
   - **ACC-6.3**: Renewal process shall allow for simplified verification if criteria unchanged
7. **ACC-7**: The system shall maintain accreditation history
   - **ACC-7.1**: Historical accreditation records shall be maintained with status changes
   - **ACC-7.2**: Documentation associated with each accreditation period shall be preserved
   - **ACC-7.3**: Audit trail of verification actions shall be recorded

3.4 Authentication

3.4.1 Description

The system shall provide secure, multi-factor authentication mechanisms that balance security requirements with user experience. Authentication will support multiple methods across web and mobile platforms.

3.4.2 Functional Requirements

1. **AUTH-1**: The system shall implement username/password authentication
   - **AUTH-1.1**: Email address shall serve as username

- **AUTH-1.2**: Passwords shall meet complexity requirements (minimum 8 characters, mix of character types)
- **AUTH-1.3**: Password hashing shall use industry-standard algorithms (bcrypt with appropriate work factor)
- **AUTH-1.4**: Password history shall prevent reuse of previous 5 passwords

2. **AUTH-2**: The system shall support multi-factor authentication (MFA)
   - **AUTH-2.1**: SMS one-time password (OTP) delivery
   - **AUTH-2.2**: Email OTP delivery as fallback
   - **AUTH-2.3**: Authenticator app integration (TOTP)
   - **AUTH-2.4**: Push notification authentication for mobile app users
   - **AUTH-2.5**: MFA shall be optional but strongly encouraged for all users
   - **AUTH-2.6**: MFA shall be mandatory for administrative users and high-value accounts
3. **AUTH-3**: The system shall implement biometric authentication for mobile app
   - **AUTH-3.1**: Support for fingerprint authentication
   - **AUTH-3.2**: Support for facial recognition where available
   - **AUTH-3.3**: Fallback authentication method when biometrics unavailable or fails
4. **AUTH-4**: The system shall implement secure session management
   - **AUTH-4.1**: Session tokens shall be securely generated using cryptographic methods
   - **AUTH-4.2**: Sessions shall expire after configurable idle timeout (default 30 minutes)
   - **AUTH-4.3**: Sessions shall have absolute timeout (default 24 hours)
   - **AUTH-4.4**: Session tokens shall be invalidated on logout or password change
   - **AUTH-4.5**: Active sessions shall be viewable and revocable by users
5. **AUTH-5**: The system shall implement account lockout protection
   - **AUTH-5.1**: Accounts shall be temporarily locked after 5 consecutive failed login attempts
   - **AUTH-5.2**: Lockout duration shall increase with repeated failures
   - **AUTH-5.3**: Notification shall be sent to user when account is locked
   - **AUTH-5.4**: Self-service unlock shall be available with appropriate verification
6. **AUTH-6**: The system shall provide secure password reset functionality
   - **AUTH-6.1**: Password reset shall require email verification
   - **AUTH-6.2**: Reset links shall expire after 1 hour
   - **AUTH-6.3**: Additional verification factor required for high-risk scenarios

- **AUTH-6.4**: Password reset shall invalidate all active sessions

7. **AUTH-7**: The system shall support "Remember Me" functionality
   - **AUTH-7.1**: Option to remain logged in on trusted devices
   - **AUTH-7.2**: Extended session with periodic revalidation
   - **AUTH-7.3**: Device fingerprinting for suspicious login detection
8. **AUTH-8**: The system shall implement OAuth 2.0 and OpenID Connect protocols
   - **AUTH-8.1**: Support for standard OAuth 2.0 flows
   - **AUTH-8.2**: JWT token issuance with appropriate claims
   - **AUTH-8.3**: Token validation and introspection endpoints
   - **AUTH-8.4**: Scope-based permission control
9. **AUTH-9**: The system shall implement Single Sign-On (SSO) functionality
   - **AUTH-9.1**: Support for SAML 2.0 protocol
   - **AUTH-9.2**: Integration with major identity providers
   - **AUTH-9.3**: User account linking with external identities

3.5 Authorization and Access Control

3.5.1 Description

The system shall implement role-based access control (RBAC) with granular permissions to ensure users can access only the functionality and data appropriate to their role and status.

3.5.2 Functional Requirements

1. **RBAC-1**: The system shall define core user roles
   - **RBAC-1.1**: Investor role with investment-focused permissions
   - **RBAC-1.2**: Issuer role with property management permissions
   - **RBAC-1.3**: Administrator role with platform management permissions
   - **RBAC-1.4**: Support role with limited administrative capabilities
   - **RBAC-1.5**: System role for automated processes
2. **RBAC-2**: The system shall implement hierarchical role structure
   - **RBAC-2.1**: Parent-child role relationships
   - **RBAC-2.2**: Permission inheritance from parent roles
   - **RBAC-2.3**: Role hierarchy management interface for administrators
3. **RBAC-3**: The system shall define granular permissions

- **RBAC-3.1**: Operation-based permissions (create, read, update, delete)
- **RBAC-3.2**: Resource-based permissions (users, properties, investments)
- **RBAC-3.3**: Permission grouping for simplified management
- **RBAC-3.4**: Custom permission definitions for specific features

4. **RBAC-4**: The system shall support role assignment and management
   - **RBAC-4.1**: Default role assignment based on user type
   - **RBAC-4.2**: Role assignment modification by administrators
   - **RBAC-4.3**: Multiple role assignment capability
   - **RBAC-4.4**: Temporary role assignments with expiration
5. **RBAC-5**: The system shall implement permission checking throughout the application
   - **RBAC-5.1**: API-level permission enforcement
   - **RBAC-5.2**: UI element visibility based on permissions
   - **RBAC-5.3**: Data filtering based on access rights
   - **RBAC-5.4**: Detailed logging of permission checks and access attempts
6. **RBAC-6**: The system shall support data-level access control
   - **RBAC-6.1**: Ownership-based access control
   - **RBAC-6.2**: Group-based sharing and permissions
   - **RBAC-6.3**: Geographical or jurisdictional restrictions
   - **RBAC-6.4**: Time-based access restrictions
7. **RBAC-7**: The system shall enforce verification status-based restrictions
   - **RBAC-7.1**: Feature access based on KYC verification status
   - **RBAC-7.2**: Investment access based on accreditation status
   - **RBAC-7.3**: Administrative notification of access attempts by unverified users

3.6 User Profile Management

3.6.1 Description

The system shall provide comprehensive user profile management capabilities, allowing users to maintain their personal information, preferences, and account settings securely.

3.6.2 Functional Requirements

1. **PROF-1**: The system shall provide profile information management
   - **PROF-1.1**: View and edit personal information (name, contact details, address)

- **PROF-1.2**: Profile completeness indicator showing required vs. optional fields
- **PROF-1.3**: Verification of critical information changes (email, phone)
- **PROF-1.4**: Change history tracking for audit purposes

2. **PROF-2**: The system shall support communication preferences management
   - **PROF-2.1**: Email notification preferences (investment updates, platform news, marketing)
   - **PROF-2.2**: SMS notification preferences
   - **PROF-2.3**: Push notification preferences for mobile app
   - **PROF-2.4**: Contact preference scheduling (time of day, frequency)
3. **PROF-3**: The system shall provide security settings management
   - **PROF-3.1**: Password change functionality
   - **PROF-3.2**: MFA enrollment and management
   - **PROF-3.3**: Trusted devices management
   - **PROF-3.4**: Login notification settings
   - **PROF-3.5**: Active sessions view and termination
4. **PROF-4**: The system shall support display and locale preferences
   - **PROF-4.1**: Language selection (English, Arabic initially, expandable)
   - **PROF-4.2**: Date and time format preferences
   - **PROF-4.3**: Currency display preferences
   - **PROF-4.4**: Accessibility settings
5. **PROF-5**: The system shall provide document management
   - **PROF-5.1**: View uploaded verification documents
   - **PROF-5.2**: Document status tracking (pending, approved, rejected)
   - **PROF-5.3**: Document replacement/update functionality
   - **PROF-5.4**: Secure document download with watermarking
6. **PROF-6**: The system shall support profile photo management
   - **PROF-6.1**: Upload and crop profile photo
   - **PROF-6.2**: Default avatar options
   - **PROF-6.3**: Automatic resizing for different UI contexts
7. **PROF-7**: The system shall provide account status management
   - **PROF-7.1**: View current account status
   - **PROF-7.2**: Request account suspension (temporary)

- **PROF-7.3**: Request account deletion with confirmation workflow
- **PROF-7.4**: Reactivation process for suspended accounts

8. **PROF-8**: The system shall maintain activity history
   - **PROF-8.1**: Login history with device and location information
   - **PROF-8.2**: Critical account changes log
   - **PROF-8.3**: Security events log (password changes, MFA changes)
   - **PROF-8.4**: Filtering and search capabilities for history

4. External Interface Requirements

4.1 User Interfaces

1. **UI-1**: Registration Interface
   - **UI-1.1**: Multi-step wizard with progress indicators
   - **UI-1.2**: Form validation with clear error messages
   - **UI-1.3**: Mobile-responsive design for all screen sizes
   - **UI-1.4**: Support for right-to-left languages (Arabic)
2. **UI-2**: Authentication Interface
   - **UI-2.1**: Login form with clear instructions
   - **UI-2.2**: Multi-factor authentication screens
   - **UI-2.3**: Password reset interface
   - **UI-2.4**: Biometric authentication on mobile
3. **UI-3**: Profile Management Interface
   - **UI-3.1**: Dashboard overview of verification status
   - **UI-3.2**: Tabbed interface for different profile sections
   - **UI-3.3**: Inline editing of profile fields
   - **UI-3.4**: Document upload interface with preview
4. **UI-4**: Administrative Interface
   - **UI-4.1**: User search and filtering
   - **UI-4.2**: Verification review dashboard
   - **UI-4.3**: User management controls
   - **UI-4.4**: Role and permission management

4.2 Hardware Interfaces

1. **HW-1**: Mobile Device Integration
    - **HW-1.1**: Camera access for document scanning and facial verification
    - **HW-1.2**: Biometric sensor access (fingerprint, facial recognition)
    - **HW-1.3**: Push notification capability
2. **HW-2**: Server Hardware Requirements
    - **HW-2.1**: Azure cloud infrastructure with appropriate scaling capabilities
    - **HW-2.2**: Hardware security modules (HSM) for cryptographic operations
    - **HW-2.3**: Load balancing for distributed traffic

4.3 Software Interfaces

1. **SW-1**: KYC/AML Service Integration
    - **SW-1.1**: RESTful API integration with selected providers
    - **SW-1.2**: Data format specifications for information exchange
    - **SW-1.3**: Error handling and fallback procedures
2. **SW-2**: Payment Gateway Integration
    - **SW-2.1**: Secure payment processing for verification fees (if applicable)
    - **SW-2.2**: Webhook handling for payment status updates
    - **SW-2.3**: Reconciliation reporting
3. **SW-3**: Communication Services Integration
    - **SW-3.1**: Email service provider integration
    - **SW-3.2**: SMS gateway integration
    - **SW-3.3**: Push notification service integration
4. **SW-4**: Internal Platform Integration
    - **SW-4.1**: Wallet system API integration
    - **SW-4.2**: Investment system API integration
    - **SW-4.3**: Property listing system API integration
    - **SW-4.4**: Reporting system integration

4.4 Communication Interfaces

1. **COM-1**: External API Communications
    - **COM-1.1**: HTTPS/TLS 1.3 for all external communications
    - **COM-1.2**: API rate limiting and throttling

- **COM-1.3**: Request/response logging and monitoring

2. **COM-2**: Mobile App Communication
   - **COM-2.1**: RESTful API endpoints optimized for mobile
   - **COM-2.2**: Compression for bandwidth optimization
   - **COM-2.3**: Offline capability with synchronization
3. **COM-3**: Notification Delivery
   - **COM-3.1**: Email delivery protocols (SMTP, API-based)
   - **COM-3.2**: SMS delivery protocols
   - **COM-3.3**: Push notification delivery for mobile

5. Non-Functional Requirements

5.1 Performance Requirements

1. **PERF-1**: Response Time
   - **PERF-1.1**: Login response time < 2 seconds (95th percentile)
   - **PERF-1.2**: Registration step submission < 3 seconds (95th percentile)
   - **PERF-1.3**: Profile updates < 3 seconds (95th percentile)
   - **PERF-1.4**: User search response time < 5 seconds (95th percentile)
2. **PERF-2**: Throughput
   - **PERF-2.1**: Support for 100+ concurrent registrations
   - **PERF-2.2**: Support for 500+ concurrent logins
   - **PERF-2.3**: Support for 10,000+ concurrent authenticated sessions
3. **PERF-3**: Scalability
   - **PERF-3.1**: Horizontal scaling for increased user load
   - **PERF-3.2**: Database partitioning strategy for large user bases
   - **PERF-3.3**: Caching strategy for frequently accessed data
4. **PERF-4**: Resource Utilization
   - **PERF-4.1**: Efficient CPU utilization under load
   - **PERF-4.2**: Memory optimization for server processes
   - **PERF-4.3**: Network bandwidth optimization for mobile clients

5.2 Security Requirements

1. **SEC-1**: Data Protection

- **SEC-1.1**: Encryption of all PII at rest using AES-256
- **SEC-1.2**: Encryption of all data in transit using TLS 1.3
- **SEC-1.3**: Secure key management with proper rotation
- **SEC-1.4**: Field-level encryption for highly sensitive data

2. **SEC-2**: Authentication Security
   - **SEC-2.1**: Password storage using bcrypt with appropriate work factor
   - **SEC-2.2**: CSRF protection for authentication endpoints
   - **SEC-2.3**: Brute force protection with progressive delays
   - **SEC-2.4**: Account lockout with notification
3. **SEC-3**: Authorization Security
   - **SEC-3.1**: Fine-grained permission checks for all operations
   - **SEC-3.2**: JWT token security with appropriate expiration
   - **SEC-3.3**: API request validation and sanitization
   - **SEC-3.4**: Principle of least privilege for all access
4. **SEC-4**: Infrastructure Security
   - **SEC-4.1**: Web Application Firewall (WAF) implementation
   - **SEC-4.2**: DDoS protection measures
   - **SEC-4.3**: Regular security scanning and penetration testing
   - **SEC-4.4**: Server hardening according to industry standards
5. **SEC-5**: Audit and Compliance
   - **SEC-5.1**: Comprehensive audit logging of security events
   - **SEC-5.2**: Log integrity protection
   - **SEC-5.3**: Compliance with industry security standards (OWASP, NIST)
   - **SEC-5.4**: Regular security compliance reviews

5.3 Reliability Requirements

1. **REL-1**: Availability
   - **REL-1.1**: System uptime of 99.9% (excluding planned maintenance)
   - **REL-1.2**: Authentication services uptime of 99.95%
   - **REL-1.3**: Planned maintenance windows with minimal disruption
2. **REL-2**: Fault Tolerance
   - **REL-2.1**: Redundancy for critical system components

- **REL-2.2**: Graceful degradation during partial system failures
- **REL-2.3**: Automatic recovery from common error conditions
- **REL-2.4**: Failover capabilities for authentication services

3. **REL-3**: Recoverability
   - **REL-3.1**: Data backup with point-in-time recovery capability
   - **REL-3.2**: Disaster recovery procedures with RPO < 1 hour
   - **REL-3.3**: Recovery time objective (RTO) < 4 hours for full system
   - **REL-3.4**: Transaction logging with replay capability
4. **REL-4**: Error Handling
   - **REL-4.1**: Comprehensive error logging with contextual information
   - **REL-4.2**: User-friendly error messages without technical details
   - **REL-4.3**: Automated error alerting for critical failures
   - **REL-4.4**: Graceful timeout handling for external service calls

5.4 Usability Requirements

1. **USE-1**: Accessibility
   - **USE-1.1**: Compliance with WCAG 2.1 Level AA standards
   - **USE-1.2**: Screen reader compatibility
   - **USE-1.3**: Keyboard navigation support
   - **USE-1.4**: Color contrast ratios meeting accessibility standards
2. **USE-2**: User Experience
   - **USE-2.1**: Intuitive navigation with clear labels and icons
   - **USE-2.2**: Consistent UI patterns across the platform
   - **USE-2.3**: Mobile-optimized interfaces with touch-friendly controls
   - **USE-2.4**: Progressive disclosure of complex features
3. **USE-3**: Internationalization
   - **USE-3.1**: Multi-language support (initially English and Arabic)
   - **USE-3.2**: Localized date, time, and number formats
   - **USE-3.3**: Right-to-left (RTL) layout support
   - **USE-3.4**: Culture-sensitive content and imagery
4. **USE-4**: Guidance and Help
   - **USE-4.1**: Contextual help and tooltips for complex fields

- **USE-4.2**: Step-by-step guidance for multi-step processes
- **USE-4.3**: Comprehensive FAQ and help documentation
- **USE-4.4**: In-app tutorials for key features

5.5 Compliance Requirements

1. **COMP-1**: Regulatory Compliance
   - **COMP-1.1**: Compliance with applicable financial regulations
   - **COMP-1.2**: KYC/AML procedures meeting regulatory standards
   - **COMP-1.3**: Securities laws compliance for investor accreditation
   - **COMP-1.4**: Regular compliance audits and documentation
2. **COMP-2**: Data Protection Compliance
   - **COMP-2.1**: GDPR compliance for EU users
   - **COMP-2.2**: CCPA compliance for California users
   - **COMP-2.3**: Data minimization and purpose limitation
   - **COMP-2.4**: Data subject rights implementation (access, deletion, etc.)
3. **COMP-3**: Record Keeping
   - **COMP-3.1**: Transaction records retention for required periods
   - **COMP-3.2**: Identity verification records retention
   - **COMP-3.3**: Audit trail preservation for compliance evidence
   - **COMP-3.4**: Secure, tamper-evident storage for compliance records
4. **COMP-4**: Reporting Compliance
   - **COMP-4.1**: Suspicious activity reporting capability
   - **COMP-4.2**: Regulatory reporting templates and generation
   - **COMP-4.3**: Compliance metrics tracking and reporting
   - **COMP-4.4**: Audit-ready reporting and documentation

6. Technical Requirements

6.1 Database Requirements

1. **DB-1**: User Data Storage
   - **DB-1.1**: Relational database schema for user profile information
   - **DB-1.2**: Efficient indexing for user lookup and filtering
   - **DB-1.3**: Data partitioning strategy for scalability

- **DB-1.4**: Database security measures including column-level encryption

2. **DB-2**: Document Storage
   - **DB-2.1**: Blob storage for identity documents and supporting files
   - **DB-2.2**: Metadata database for document indexing and retrieval
   - **DB-2.3**: Versioning support for document updates
   - **DB-2.4**: Document lifecycle management with retention policies
3. **DB-3**: Audit and Log Storage
   - **DB-3.1**: Structured logging system with search capabilities
   - **DB-3.2**: Immutable audit trail for security and compliance events
   - **DB-3.3**: Performance-optimized log ingestion and query
   - **DB-3.4**: Log rotation and archiving processes
4. **DB-4**: Performance and Scaling
   - **DB-4.1**: Caching layer for frequently accessed user data
   - **DB-4.2**: Read replicas for reporting and analytics queries
   - **DB-4.3**: Database performance monitoring and optimization
   - **DB-4.4**: Automated backup and recovery procedures

6.2 API Requirements

1. **API-1**: API Architecture
   - **API-1.1**: RESTful API design following industry best practices
   - **API-1.2**: API versioning strategy
   - **API-1.3**: Consistent resource naming conventions
   - **API-1.4**: HTTP method usage aligned with standard semantics
2. **API-2**: API Security
   - **API-2.1**: OAuth 2.0 token-based authentication
   - **API-2.2**: Scope-based authorization for API endpoints
   - **API-2.3**: Rate limiting and throttling for API abuse prevention
   - **API-2.4**: Input validation and sanitization for all API inputs
3. **API-3**: API Documentation
   - **API-3.1**: OpenAPI (Swagger) specification for all endpoints
   - **API-3.2**: Detailed method documentation including parameters and responses
   - **API-3.3**: Error code documentation and handling instructions

- **API-3.4**: Code examples for common API operations

4. **API-4**: Mobile API Considerations
   - **API-4.1**: Optimization for mobile bandwidth constraints
   - **API-4.2**: Batch operations to reduce API calls
   - **API-4.3**: Pagination for large data sets
   - **API-4.4**: Offline operation support with synchronization

6.3 Integration Requirements

1. **INT-1**: KYC/AML Integration
   - **INT-1.1**: Integration with selected KYC provider API
   - **INT-1.2**: Secure document transmission protocols
   - **INT-1.3**: Webhook handling for asynchronous verification results
   - **INT-1.4**: Fallback procedures for service unavailability
2. **INT-2**: Communication Services Integration
   - **INT-2.1**: Email service provider integration with templates
   - **INT-2.2**: SMS gateway integration for verification codes and alerts
   - **INT-2.3**: Push notification service integration for mobile app
   - **INT-2.4**: Delivery status tracking and failure handling
3. **INT-3**: Internal System Integration
   - **INT-3.1**: Integration with wallet system for user account linking
   - **INT-3.2**: Integration with investment system for eligibility verification
   - **INT-3.3**: Integration with property listing system for access control
   - **INT-3.4**: Integration with reporting system for analytics and compliance
4. **INT-4**: Third-Party Authentication Providers
   - **INT-4.1**: Integration with OAuth providers (Google, Apple, etc.)
   - **INT-4.2**: Account linking functionality for external identities
   - **INT-4.3**: Fallback authentication methods
   - **INT-4.4**: Security monitoring for third-party authentication

6.4 Mobile Application Requirements

1. **MOB-1**: Flutter Implementation
   - **MOB-1.1**: Cross-platform implementation using Flutter framework

- **MOB-1.2**: Native module integration for device-specific features
- **MOB-1.3**: Responsive UI adapting to different screen sizes
- **MOB-1.4**: Platform-specific UI guidelines adherence

2. **MOB-2**: Offline Functionality
   - **MOB-2.1**: Local data storage for key user information
   - **MOB-2.2**: Offline authentication capability with local token validation
   - **MOB-2.3**: Queue system for operations during connectivity loss
   - **MOB-2.4**: Synchronization protocol when connectivity restored
3. **MOB-3**: Mobile Security
   - **MOB-3.1**: Secure local storage with encryption
   - **MOB-3.2**: Certificate pinning for API communications
   - **MOB-3.3**: Jailbreak/root detection
   - **MOB-3.4**: Secure biometric integration
   - **MOB-3.5**: Screen security for sensitive information
4. **MOB-4**: Mobile Performance
   - **MOB-4.1**: Optimization for low-end devices
   - **MOB-4.2**: Battery usage optimization
   - **MOB-4.3**: Bandwidth conservation techniques
   - **MOB-4.4**: Cold start time optimization

7. System Administration Requirements

7.1 User Administration

1. **ADMIN-1**: User Management
   - **ADMIN-1.1**: Administrative interface for user search and filtering
   - **ADMIN-1.2**: User detail view with complete profile information
   - **ADMIN-1.3**: User status management (activate, suspend, delete)
   - **ADMIN-1.4**: Administrative password reset capability
2. **ADMIN-2**: Verification Management
   - **ADMIN-2.1**: KYC verification review and approval interface
   - **ADMIN-2.2**: Document review tools with zoom and annotation
   - **ADMIN-2.3**: Verification status override capabilities

- **ADMIN-2.4**: Verification history tracking

3. **ADMIN-3**: Role and Permission Management
   - **ADMIN-3.1**: Role creation and modification interface
   - **ADMIN-3.2**: Permission assignment to roles
   - **ADMIN-3.3**: User role assignment interface
   - **ADMIN-3.4**: Role hierarchy visualization and management
4. **ADMIN-4**: Bulk Operations
   - **ADMIN-4.1**: Bulk user import functionality
   - **ADMIN-4.2**: Bulk status updates
   - **ADMIN-4.3**: Bulk communication capability
   - **ADMIN-4.4**: Bulk operation audit logging

7.2 System Monitoring and Maintenance

1. **MON-1**: Performance Monitoring
   - **MON-1.1**: Real-time performance metrics dashboard
   - **MON-1.2**: Performance threshold alerts
   - **MON-1.3**: Historical performance trending
   - **MON-1.4**: Resource utilization monitoring
2. **MON-2**: Security Monitoring
   - **MON-2.1**: Failed login attempt monitoring
   - **MON-2.2**: Suspicious activity detection
   - **MON-2.3**: API usage anomaly detection
   - **MON-2.4**: Security incident alerts and reporting
3. **MON-3**: System Maintenance
   - **MON-3.1**: Scheduled maintenance planning tools
   - **MON-3.2**: Zero-downtime deployment capability
   - **MON-3.3**: Database maintenance utilities
   - **MON-3.4**: Cache invalidation and refresh tools
4. **MON-4**: Debugging and Troubleshooting
   - **MON-4.1**: Detailed logging with log level configuration
   - **MON-4.2**: User session replay for issue reproduction
   - **MON-4.3**: Error tracking and correlation

- **MON-4.4**: System health check endpoints

7.3 Reporting and Analytics

1. **REP-1**: User Analytics
   - **REP-1.1**: Registration funnel analysis
   - **REP-1.2**: Verification completion rates and times
   - **REP-1.3**: User activity and engagement metrics
   - **REP-1.4**: User demographic and segmentation reporting
2. **REP-2**: Operational Reporting
   - **REP-2.1**: KYC verification processing metrics
   - **REP-2.2**: Authentication metrics (success rates, failures)
   - **REP-2.3**: API usage statistics
   - **REP-2.4**: Performance and availability reporting
3. **REP-3**: Compliance Reporting
   - **REP-3.1**: Suspicious activity reports
   - **REP-3.2**: Verification status reporting
   - **REP-3.3**: Audit trail reports for compliance review
   - **REP-3.4**: Regulatory submission report generation
4. **REP-4**: Custom Reporting
   - **REP-4.1**: Report builder interface for ad-hoc reports
   - **REP-4.2**: Scheduled report generation and distribution
   - **REP-4.3**: Report export in multiple formats (CSV, PDF, Excel)
   - **REP-4.4**: Data visualization tools for key metrics

8. Implementation Approach

8.1 Development Methodology

The User Registration and Authentication component will be developed using an Agile methodology with two-week sprints. The development process will follow the principles outlined in the Development Approach document:

1. Quality-first development with automated testing
2. Security integration throughout the development lifecycle
3. Regular stakeholder reviews and feedback incorporation

4. Incremental delivery with prioritized feature implementation

8.2 Technical Approach

1. **Backend Implementation**
   - ASP.NET Core 8 backend with clean architecture principles
   - Entity Framework Core for data access
   - IdentityServer4 for authentication and authorization
   - MediatR for implementing CQRS pattern
   - Azure Service Bus for asynchronous messaging
2. **Frontend Implementation**
   - React-based web frontend with responsive design
   - Flutter-based mobile application with shared business logic
   - Shared component library for consistent UI
   - Accessibility-first approach to UI development
3. **Testing Strategy**
   - Unit testing with xUnit, Moq, and FluentAssertions
   - Integration testing of API endpoints
   - End-to-end testing of critical user flows
   - Performance testing for load and stress scenarios
   - Security testing with automated and manual penetration testing
4. **Deployment Strategy**
   - CI/CD pipeline using Azure DevOps
   - Infrastructure as Code using Terraform and ARM templates
   - Blue-green deployment for zero-downtime updates
   - Automated rollback capability for failed deployments

9. Acceptance Criteria

The following criteria will be used to determine the acceptance of the User Registration and Authentication component:

9.1 Functional Acceptance Criteria

1. **Registration Flow**
   - Complete user registration flow works end-to-end for all user types

- Email and phone verification processes function correctly
- All required user information is collected and stored properly
- Registration completion rate meets or exceeds 95% target

2. **KYC/AML Verification**
   - Integration with KYC provider successfully verifies user identities
   - Document upload and verification process works as specified
   - Verification status tracking and updates function correctly
   - Verification processing times meet performance requirements
3. **Authentication System**
   - All authentication methods function correctly (password, MFA, biometric)
   - Session management adheres to security requirements
   - Password policies and account security features work as specified
   - Authentication success rates meet performance targets
4. **Profile Management**
   - Users can successfully update profile information
   - Settings and preferences are correctly stored and applied
   - Document management functions work as specified
   - Activity history and logs are accurately recorded

9.2 Non-Functional Acceptance Criteria

1. **Performance**
   - System handles specified user load without degradation
   - Response times meet or exceed performance requirements
   - System scales appropriately with increased load
2. **Security**
   - System passes security penetration testing
   - Encryption implementation meets security standards
   - No critical or high-severity security vulnerabilities
   - Compliance with all specified security requirements
3. **Reliability**
   - System meets uptime requirements during testing period
   - Fault tolerance capabilities demonstrated through failure testing

- Data integrity maintained during failure scenarios
- Backup and recovery processes function correctly

4. **Usability**
   - User feedback indicates intuitive and clear interfaces
   - Accessibility testing confirms WCAG 2.1 AA compliance
   - Mobile interfaces function correctly across device types
   - Help and guidance features provide adequate support

10. Testing Requirements

10.1 Test Types

1. **Unit Testing**
   - Test coverage of at least 80% for core business logic
   - All critical paths and edge cases covered
   - Test automation integrated into CI/CD pipeline
   - Unit test results required for build promotion

2. **Integration Testing**
   - API endpoint testing for all exposed interfaces
   - Database integration testing
   - Third-party service integration testing
   - Error handling and resilience testing

3. **System Testing**
   - End-to-end testing of complete user flows
   - Cross-browser and cross-device testing
   - Negative testing scenarios
   - Data validation and integrity testing

4. **Performance Testing**
   - Load testing under expected and peak conditions
   - Stress testing to identify breaking points
   - Endurance testing for sustained operations
   - Scalability testing with increasing user loads

5. **Security Testing**

- Vulnerability scanning and penetration testing
- Authentication and authorization testing
- Data protection testing
- Common attack vector testing (OWASP Top 10)

6. **Usability Testing**
   - User acceptance testing with representative users
   - Accessibility testing with screen readers and tools
   - Mobile usability testing on various devices
   - International usability testing for localization

10.2 Test Environments

1. **Development Environment**
   - Individual developer environments
   - Local testing capabilities
   - Mocked external dependencies
2. **Integration Environment**
   - Continuous integration environment
   - Shared database with test data
   - Test instances of third-party services where possible
3. **QA Environment**
   - Stable environment for manual and automated testing
   - Complete environment with all dependencies
   - Data reset capabilities for test isolation
4. **Staging Environment**
   - Production-like environment for final validation
   - Performance testing environment
   - Security testing environment

11. Data Migration and Transition

11.1 Data Migration Requirements

1. **Initial Data Setup**
   - Reference data for dropdown lists and lookups

- System configuration data
- Test user accounts for various scenarios

2. **Migration Approach**
   - No legacy data migration required for initial implementation
   - Future migration capabilities to be considered in design
   - Data import utilities for bulk user creation

11.2 Transition Requirements

1. **Deployment Approach**
   - Phased rollout starting with core authentication features
   - Incremental addition of enhanced verification features
   - Beta testing program with selected users

2. **Training Requirements**
   - Administrator training for user management
   - Compliance team training for verification processes
   - Support team training for troubleshooting common issues
   - End-user documentation and guided tutorials

3. **Cutover Planning**
   - Go-live checklist with verification steps
   - Rollback procedures in case of critical issues
   - Post-deployment monitoring plan
   - Support escalation procedures for launch period

12. System Architecture

12.1 Architecture Overview

The User Registration and Authentication component will utilize a layered architecture following clean architecture principles to ensure separation of concerns, testability, and maintainability.

![Architecture Diagram Placeholder]

The system will consist of the following architectural layers:

1. **Presentation Layer**
   - Web interface (React)

- Mobile interface (Flutter)
- API controllers

2. **Application Layer**
   - Application services
   - Command/query handlers (CQRS pattern)
   - Input validation
   - Integration with external services
3. **Domain Layer**
   - Business entities and logic
   - Domain services
   - Business rules and validation
4. **Infrastructure Layer**
   - Data access using Entity Framework Core
   - External service clients
   - Authentication services (IdentityServer4)
   - Logging and monitoring implementation
   - Message bus integration

12.2 Component Interactions

1. **User Registration Flow**
   - Web/mobile UI collects registration data
   - API validates input and creates user record
   - Background process initiates verification
   - Email/SMS service sends verification messages
   - Webhook handler processes verification results
2. **Authentication Flow**
   - User provides credentials
   - Authentication service validates credentials
   - Token service issues JWT token with claims
   - Authorization middleware validates tokens for protected resources
   - Session service manages active sessions

3. **KYC Verification Flow**
    - User uploads verification documents
    - Document service processes and encrypts documents
    - Integration service sends verification request to KYC provider
    - Webhook receiver processes verification result
    - Notification service informs user of outcome
4. **User Profile Management Flow**
    - User requests profile information
    - Authorization service validates access rights
    - Profile service retrieves and returns data
    - Updates processed through validation pipeline
    - Audit service logs significant changes

12.3 Deployment Architecture

The system will be deployed on Microsoft Azure using containerized services for scalability and maintainability:

1. **Web Tier**
    - Azure App Service for web application
    - Azure CDN for static content
    - Azure Front Door for global load balancing and WAF
2. **API Tier**
    - Azure Kubernetes Service (AKS) for API services
    - Container instances with auto-scaling
    - API Management for gateway and monitoring
3. **Data Tier**
    - Azure SQL Database for relational data
    - Azure Redis Cache for distributed caching
    - Azure Blob Storage for document storage
    - Azure Cosmos DB for high-throughput logging
4. **Supporting Services**
    - Azure Service Bus for messaging
    - Azure Key Vault for secrets management

- Azure Application Insights for monitoring
- Azure Active Directory B2C for identity management

13. Security and Privacy

13.1 Security Architecture

1. **Defense in Depth**
   - Multiple security layers throughout the application
   - Security controls at network, host, application, and data levels
   - Regular security assessments and penetration testing
   - Continuous vulnerability monitoring
2. **Identity Security**
   - Strong password policies and secure storage
   - Multi-factor authentication implementation
   - Account lockout and anti-brute force protections
   - Session management with appropriate timeouts
3. **Data Security**
   - Encryption of data at rest (AES-256)
   - Encryption of data in transit (TLS 1.3)
   - Field-level encryption for highly sensitive data
   - Secure key management with rotation policies
4. **API Security**
   - OAuth 2.0 and OpenID Connect implementation
   - JWT token security with appropriate signing
   - API request validation and sanitization
   - Rate limiting and throttling for abuse prevention

13.2 Privacy Controls

1. **Data Minimization**
   - Collection of only necessary personal information
   - Purpose-specific data collection with clear disclosure
   - Retention periods defined for different data types
   - Automated data purging after retention period

2. **User Consent**
    - Clear consent collection during registration
    - Granular consent options for different data uses
    - Consent withdrawal mechanisms
    - Consent record keeping for audit purposes
3. **Data Subject Rights**
    - Access to personal data functionality
    - Data portability in standard formats
    - Data correction mechanisms
    - Right to erasure implementation with verification
4. **Privacy by Design**
    - Privacy impact assessments during development
    - Default privacy-preserving settings
    - Anonymization for analytics and reporting
    - Privacy-enhancing technologies implementation

14. Documentation Requirements

14.1 Development Documentation

1. **Architecture Documentation**
    - System architecture overview
    - Component diagrams and interactions
    - Data models and relationships
    - Security architecture
2. **API Documentation**
    - OpenAPI (Swagger) documentation
    - API usage examples
    - Authentication and authorization details
    - Error codes and handling
3. **Code Documentation**
    - Inline code documentation
    - Class and method documentation

- Business logic explanation
- Code examples for complex processes

4. **Database Documentation**
   - Database schema documentation
   - Entity-relationship diagrams
   - Stored procedures and functions
   - Index strategy and optimization

14.2 Operational Documentation

1. **Deployment Guides**
   - Environment setup instructions
   - Deployment procedures
   - Configuration parameters
   - Scaling guidelines

2. **Administration Guides**
   - User management procedures
   - Verification process management
   - System monitoring instructions
   - Troubleshooting procedures

3. **Security Documentation**
   - Security controls overview
   - Security incident response procedures
   - Audit logging and review guidelines
   - Compliance verification procedures

4. **Maintenance Documentation**
   - Backup and recovery procedures
   - Performance tuning guidelines
   - Database maintenance procedures
   - System update guidelines

14.3 End-User Documentation

1. **User Guides**

- Registration process guide
- KYC verification guide
- Account management guide
- Security best practices guide

2. **Help Content**
   - Contextual help for complex fields
   - Frequently asked questions (FAQ)
   - Troubleshooting guides
   - Video tutorials for key processes
3. **Mobile App Documentation**
   - Mobile app installation guide
   - Mobile-specific features guide
   - Offline functionality explanation
   - Mobile security guide
4. **Administrator User Guides**
   - User management procedures
   - Verification review procedures
   - Reporting and analytics guides
   - System configuration guide

15. Glossary

Term	Definition
API	Application Programming Interface; a set of rules that allow programs to talk to each other
Authentication	The process of verifying the identity of a user or system
Authorization	The process of determining whether a user has permission to access a resource
CCPA	California Consumer Privacy Act; data privacy law that applies to businesses serving California residents
CQRS	Command Query Responsibility Segregation; a pattern separating read and write operations
GDPR	General Data Protection Regulation; EU data protection and privacy regulation
JWT	JSON Web Token; a compact, URL-safe means of representing claims between two parties
KYC/AML	Know Your Customer/Anti-Money Laundering; regulatory processes for verifying client identity and preventing illegal activities
MFA	Multi-Factor Authentication; authentication method requiring two or more verification factors
OAuth	Open Authorization; an open standard for access delegation
OTP	One-Time Password; a password valid for only one login session
PEP	Politically Exposed Person; an individual with prominent public functions
PII	Personally Identifiable Information; data that could identify a specific individual
RBAC	Role-Based Access Control; approach to restricting system access based on roles
REST	Representational State Transfer; architectural style for distributed systems
SSO	Single Sign-On; authentication process allowing a user to access multiple applications with one set of credentials
TLS	Transport Layer Security; cryptographic protocol designed to provide communications security
TOTP	Time-based One-Time Password; temporary passcode that uses current time as a source of uniqueness
UI/UX	User Interface/User Experience; the visual elements and interaction experience of software
WCAG	Web Content Accessibility Guidelines; recommendations for making web content accessible

Appendices

Appendix A: Related Documents

1. Project Charter (project-charter.docx)
2. Development Approach and Tech Stack (development-approach.docx)
3. Feature Comparison with Similar Platforms (emtelaak-feature-comparison.docx)
4. User Registration Flow (User Registration flow.pdf)
5. User Registration and Authentication BRD v1.0 (user-registration-brd.docx)

Appendix B: Approval

This Software Requirements Specification has been reviewed and approved by the following stakeholders:

Name	Role	Signature	Date
	Product Owner		
	Technical Architect		
	Project Manager		
	QA Lead		
	Security Officer		

Appendix C: UI Wireframes

This appendix contains wireframes for key user interfaces in the User Registration and Authentication system. These wireframes represent the conceptual design and layout of main screens and should be used as a reference for UI development.

C.1 User Registration Flow

C.1.1 Registration Step 1: Basic Information

![Registration Step 1 Wireframe]

This screen collects initial user information:

- Email address field with validation
- Password field with strength indicator
- Password confirmation field
- Full name fields (First, Last)
- Phone number field with country code selector
- User type selection (radio buttons or dropdown)
- "Next" button (disabled until form is valid)
- Link to Login page for existing users

References: REG-1.1, REG-2.1, REG-2.2, REG-2.3, REG-2.4, REG-2.5

C.1.2 Registration Step 2: Email Verification

![Email Verification Wireframe]

This screen guides the user through email verification:

- Instructional text explaining the process
- Email address display (non-editable)
- "Resend Email" button
- Timer showing when resend is available
- Input field for verification code (optional approach)
- "Verify" button
- Option to change email address

References: REG-3.1, REG-3.2, REG-3.3

C.1.3 Registration Step 3: Phone Verification

![Phone Verification Wireframe]

This screen handles phone number verification:

- Phone number display (non-editable)
- SMS code input fields (separate boxes for each digit)
- "Resend Code" button with timer
- "Verify" button
- Option to change phone number

References: REG-4.1, REG-4.2, REG-4.3

C.1.4 Registration Step 4: Terms Acceptance

![Terms Acceptance Wireframe]

This screen presents terms and privacy policy:

- Scrollable terms of service text box
- Scrollable privacy policy text box
- Checkbox for terms acceptance (unchecked by default)
- Checkbox for privacy policy acceptance (unchecked by default)
- "Next" button (disabled until both checkboxes are checked)
- "Back" button

References: REG-5.1, REG-5.2, REG-5.3

C.1.5 Registration Step 5: Additional Information

![Additional Information Wireframe]

This screen collects user-type specific information:

- Form fields specific to selected user type (Individual Investor shown):
  - Date of birth (calendar selector)
  - Nationality (dropdown)
  - Residential address fields (street, city, state, postal code, country)
  - Employment status (dropdown)
  - Employment information fields (conditional based on status)
- "Next" button
- "Back" button
- Progress indicator showing completion percentage

References: REG-6.1, REG-6.2, REG-6.3

C.1.6 Registration Step 6: Document Upload

![Document Upload Wireframe]

This screen facilitates identity document uploads:

- Document type selector (dropdown: Passport, National ID, Driver's License)
- Document upload area with drag-and-drop functionality
- "Browse Files" button
- Preview area for uploaded documents
- Document status indicator (uploading, processing, accepted)
- "Next" button (disabled until required documents are uploaded)
- "Back" button

References: REG-7.1, REG-7.2, REG-7.3, REG-7.4

C.1.7 Registration Completion

![Registration Completion Wireframe]

This screen confirms successful registration:

- Success message with checkmark icon

- Account creation confirmation
- Next steps information
- Verification status explanation
- "Go to Dashboard" button
- "Complete Profile" button (if applicable)

References: REG-8.1, REG-8.2, REG-8.3

C.2 Authentication Interfaces

C.2.1 Login Screen

![Login Screen Wireframe]

Main login interface:

- Logo and branding elements
- Email field
- Password field with show/hide toggle
- "Remember Me" checkbox
- "Forgot Password" link
- "Login" button
- "Register" link for new users
- Social login options (if applicable)

References: AUTH-1.1, AUTH-1.2, AUTH-1.3, AUTH-7.1

C.2.2 Multi-Factor Authentication

![MFA Screen Wireframe]

MFA verification screen:

- Instructional text explaining the process
- Visual indicator of MFA method (SMS, Email, Authenticator app)
- Code input fields
- "Resend Code" button with timer
- "Verify" button
- "Use Another Method" link

- "Cancel" button

References: AUTH-2.1, AUTH-2.2, AUTH-2.3, AUTH-2.4

C.2.3 Biometric Authentication (Mobile)

![Biometric Authentication Wireframe]

Mobile biometric authentication screen:

- Biometric prompt (fingerprint or facial recognition)
- Animation indicating scan in progress
- "Use Password Instead" option
- Success/failure indication

References: AUTH-3.1, AUTH-3.2, AUTH-3.3

C.2.4 Password Reset

![Password Reset Wireframe]

Password reset request screen:

- Instructional text
- Email input field
- "Send Reset Link" button
- "Back to Login" link

Password reset completion screen:

- New password field with strength indicator
- Confirm password field
- Password requirements list with real-time validation indicators
- "Reset Password" button

References: AUTH-6.1, AUTH-6.2, AUTH-6.3, AUTH-6.4

C.3 User Profile Management

C.3.1 Profile Dashboard

![Profile Dashboard Wireframe]

Main profile overview screen:

- Profile completion meter
- Verification status indicators (KYC, accreditation)
- Profile photo with upload/change option
- Quick edit buttons for key information
- Navigation tabs to different profile sections
- Action buttons for common tasks

References: PROF-1.1, PROF-1.2, PROF-1.3, PROF-6.1

C.3.2 Personal Information Section

![Personal Information Wireframe]

Personal details editing interface:

- Editable fields for personal information
- Save/Cancel buttons for each section
- Change history access link
- Field validation with inline error messages
- Required field indicators

References: PROF-1.1, PROF-1.3, PROF-1.4

C.3.3 Security Settings

![Security Settings Wireframe]

Security configuration interface:

- Password change section
- Multi-factor authentication setup/management
- List of active sessions with details and "Revoke" buttons
- Login notification settings
- Recent security activity log

References: PROF-3.1, PROF-3.2, PROF-3.3, PROF-3.4, PROF-3.5

C.3.4 Communication Preferences

![Communication Preferences Wireframe]

Notification settings interface:

- Email notification toggles by category
- SMS notification toggles
- Push notification settings
- Communication frequency options
- "Save Changes" button

References: PROF-2.1, PROF-2.2, PROF-2.3, PROF-2.4

C.3.5 Document Management

![Document Management Wireframe]

Document management interface:

- Document categories tabs
- List of uploaded documents with status indicators
- Preview thumbnails
- Download/replace buttons
- Upload new document button
- Document history access

References: PROF-5.1, PROF-5.2, PROF-5.3, PROF-5.4

C.4 Administration Interfaces

C.4.1 User Management Dashboard

![User Management Dashboard Wireframe]

Administrative user management screen:

- User search with multiple filters
- User list with key information columns
- Quick action buttons (view, edit, suspend)
- Batch action dropdown
- User statistics summary

- Export options

References: ADMIN-1.1, ADMIN-1.2, ADMIN-1.3, ADMIN-1.4

C.4.2 KYC Verification Review

Verification review interface:

- User details summary
- Document viewer with zoom/pan controls
- Side-by-side comparison of ID photo and selfie
- Data extracted from documents (for verification)
- User-provided information fields
- Verification result buttons (Approve, Reject, Request More Info)
- Notes/reason field
- Previous/Next user navigation

References: ADMIN-2.1, ADMIN-2.2, ADMIN-2.3, ADMIN-2.4

C.4.3 Role Management

Role configuration interface:

- Role list with description and user count
- Role creation/edit form
- Permission assignment matrix
- Role hierarchy visualization
- Role assignment to users interface
- Search and filter capabilities

References: ADMIN-3.1, ADMIN-3.2, ADMIN-3.3, ADMIN-3.4

C.4.4 System Monitoring Dashboard

System monitoring interface:

- Real-time metrics graphs (users, logins, registrations)
- System health indicators
- Recent alerts and notifications
- Performance metrics
- User activity heat map
- Detailed metrics selection and filtering
- Date range selector

References: MON-1.1, MON-1.2, MON-1.3, MON-1.4, MON-2.1

C.5 Mobile Application Interfaces

C.5.1 Mobile Login

Mobile app login screen:

- App logo and branding
- Email/username field
- Password field with show/hide option
- "Remember Me" option
- Biometric login button
- "Forgot Password" link
- "Login" button
- "Create Account" link

References: MOB-1.3, MOB-1.4, MOB-3.4

C.5.2 Mobile Registration

Mobile registration screens:

- Step indicator showing progress
- Form fields optimized for mobile input
- Next/Back navigation
- Camera access for document scanning

- Simplified layout with progressive disclosure

References: MOB-1.1, MOB-1.3, MOB-3.1

C.5.3 Mobile Profile Management

Mobile profile interface:

- Profile header with photo and key information
- Card-based layout for different profile sections
- Quick actions floating button
- Pull-to-refresh functionality
- Offline indicator when working without connection
- Sync status for changes made offline

References: MOB-2.1, MOB-2.3, MOB-2.4, MOB-4.3

Note: These wireframes are conceptual representations of the user interfaces. Final implementations may vary based on detailed design specifications, usability testing feedback, and technical constraints. High-fidelity mockups and interactive prototypes will be developed during the UI/UX design phase.

[In a complete SRS document, actual wireframe images would be included in place of the image placeholders.]