Software Requirements Specification (SRS)

Virtual Card Financial System

Executive Summary

This Software Requirements Specification document outlines the comprehensive requirements for developing a virtual card financial system tailored for the Cameroon market. The system will provide secure, accessible, and compliant digital payment solutions to Cameroonians, enabling seamless financial transactions through mobile applications. The platform will integrate with local and international payment networks while adhering to regulatory requirements set by the Bank of Cameroon (BEAC) and the National Financial Intelligence Unit (CELLULE DE RENSEIGNEMENTS FINANCIERS - CRF).

The virtual card system addresses critical gaps in Cameroon's financial inclusion landscape, where approximately 62% of the adult population remains unbanked despite increasing mobile penetration rates exceeding 80%. This solution leverages mobile-first architecture to serve both urban and rural populations across the country's diverse telecommunications infrastructure.

1. Introduction

1.1 Purpose

The Virtual Card Financial System is designed to provide Cameroonians with secure, convenient, and accessible digital payment solutions. The system enables users to create virtual payment cards directly from their mobile devices, facilitating online and offline transactions without requiring traditional bank accounts or physical card infrastructure.

1.2 Scope

The system encompasses the following core functionalities:

- **User Authentication and Account Management** - Secure registration, login, and profile management for individual users and merchants
- **Know Your Customer (KYC) Verification** - Compliance with BEAC KYC requirements for user identity verification
- **Virtual Card Provisioning** - Creation, management, and lifecycle of virtual payment cards
- **Payment Processing** - Integration with international payment gateways and local payment networks
- **Fraud Detection and Prevention** - Real-time monitoring and prevention of fraudulent transactions
- **Transaction History and Reporting** - Comprehensive transaction records and financial reporting
- **Notifications and Alerts** - Real-time SMS and push notifications for transaction updates
- **Customer Support** - In-app support, FAQ, and escalation mechanisms

1.3 Definitions and Acronyms

Term	Definition
BEAC	Banque des États de l'Afrique Centrale (Central Bank of Central African States)
CRF	Cellule de Renseignements Financiers (National Financial Intelligence Unit)
KYC	Know Your Customer - Identity verification requirements

Term	Definition
AML	Anti-Money Laundering - Compliance framework
CFT	Combating the Financing of Terrorism - Regulatory requirement
USSD	Unstructured Supplementary Service Data - SMS-based banking protocol
OTP	One-Time Password - Authentication mechanism
JWT	JSON Web Token - Authentication token format
PCI-DSS	Payment Card Industry Data Security Standard
FCFA	Central African CFA Franc - Currency of Cameroon
IMEI	International Mobile Equipment Identity
SIM	Subscriber Identity Module

1.4 Document Organization

This SRS document is organized into the following sections:

1. **Introduction** - Purpose, scope, and definitions
2. **Overall Description** - System context and user characteristics
3. **Specific Requirements** - Functional and non-functional requirements
4. **System Architecture** - High-level system design and components
5. **Regulatory Compliance** - BEAC, CRF, and AML/CFT requirements
6. **Security Requirements** - Data protection and security measures
7. **Performance Requirements** - System performance and scalability targets
8. **Interface Requirements** - User interface and API specifications
9. **Testing Requirements** - Quality assurance and testing strategies
10. **Deployment and Maintenance** - Deployment plan and ongoing support

2. Overall Description

2.1 Product Perspective

The Virtual Card Financial System operates as a standalone mobile application with backend services that integrate with multiple external systems. The system architecture follows a microservices pattern with the following key integration points:

- **Mobile Client** - iOS and Android applications serving as the primary user interface
- **API Gateway** - Central routing and authentication layer for all client requests
- **Authentication Service** - Secure user authentication and session management
- **User Management Service** - Profile and account management
- **KYC Service** - Identity verification and compliance checks
- **Card Provisioning Service** - Virtual card creation and management
- **Payment Processing Service** - Transaction processing and settlement
- **Fraud Detection Service** - Real-time fraud monitoring and prevention
- **Notification Service** - SMS and push notification delivery
- **Database Layer** - Persistent data storage with encryption
- **Cache Layer** - Redis-based caching for performance optimization
- **External Integrations** - Payment gateways, KYC providers, and SMS services

2.2 User Classes and Characteristics

2.2.1 Individual Users (Primary Users)

Profile: Cameroonians aged 18 and above with mobile devices and basic digital literacy

Characteristics:

- Diverse technical proficiency levels (from basic to advanced)
- Limited access to traditional banking infrastructure in rural areas
- High mobile phone penetration (80%+)
- Preference for mobile-first solutions
- Concern about transaction security and fraud
- Limited data connectivity in some regions

Key Needs:

- Easy account creation without extensive documentation
- Fast and secure payment processing
- Low transaction fees
- 24/7 access to financial services
- Transaction history and receipts
- Customer support in French and English

2.2.2 Merchants and Business Users

Profile: Small to medium-sized businesses requiring payment acceptance solutions

Characteristics:

- Operate in retail, e-commerce, and services sectors
- Limited technical support infrastructure
- Require transaction reporting and settlement
- Need fraud protection and chargeback management

Key Needs:

- Easy merchant onboarding
- Real-time payment settlement
- Comprehensive transaction reporting
- Competitive transaction fees
- Integration with point-of-sale systems
- Multi-currency support

2.2.3 Administrators and Support Staff

Profile: Internal team members managing system operations and customer support

Characteristics:

- Require access to administrative dashboards
- Need user management and transaction monitoring capabilities
- Must comply with audit and regulatory requirements

Key Needs:

- Real-time system monitoring
- User management tools
- Transaction audit trails
- Compliance reporting
- Incident management

2.3 Operating Environment

2.3.1 Mobile Platforms

- **iOS:** Version 12.0 and above
- **Android:** Version 8.0 and above
- **Minimum Device RAM:** 2 GB
- **Minimum Storage:** 100 MB available space

2.3.2 Network Connectivity

- **Primary:** 4G/LTE networks (available in major urban centers)
- **Secondary:** 3G networks (nationwide coverage)
- **Fallback:** USSD for basic transactions in low-connectivity areas
- **Bandwidth Requirements:** Minimum 512 kbps for basic operations

2.3.3 Backend Infrastructure

- **Server Environment:** Cloud-based infrastructure (AWS, Google Cloud, or local hosting)
- **Database:** PostgreSQL or MySQL for relational data
- **Cache:** Redis for session and data caching
- **Message Queue:** RabbitMQ or Kafka for asynchronous processing
- **Monitoring:** ELK Stack or Datadog for system monitoring

2.3.4 External Services

- **SMS Provider:** Local Cameroon SMS gateway (e.g., Africastalking, Twilio)
- **KYC Provider:** Third-party identity verification service
- **Payment Gateway:** International payment processor (e.g., Stripe, Flutterwave)
- **Card Provisioning:** Third-party card issuance platform

2.4 Design and Implementation Constraints

2.4.1 Regulatory Constraints

- **BEAC Compliance:** System must comply with BEAC guidelines for digital financial services
- **CRF Requirements:** Anti-money laundering and counter-terrorism financing requirements
- **Data Residency:** User data must be stored within BEAC member states or with explicit regulatory approval
- **Licensing:** Operator must obtain necessary licenses from BEAC for financial services

2.4.2 Technical Constraints

- **Mobile-First Design:** Primary interface must be optimized for mobile devices
- **Low Bandwidth Support:** System must function efficiently with limited bandwidth
- **Offline Capability:** Basic functionality must work in offline mode with sync capability
- **Language Support:** System must support French and English interfaces
- **Accessibility:** WCAG 2.1 AA compliance for accessibility standards

2.4.3 Business Constraints

- **Cost Efficiency:** Transaction fees must be competitive with existing payment solutions
- **Scalability:** System must support 100,000+ concurrent users
- **Performance:** Transaction processing must complete within 30 seconds
- **Availability:** 99.9% uptime requirement for production systems

3. Specific Requirements

3.1 Functional Requirements

3.1.1 User Authentication and Account Management

FR-1.1: User Registration

- System shall allow users to register with email address or phone number
- System shall validate email format and phone number format (Cameroon +237 format)
- System shall send OTP verification code via SMS or email
- System shall require users to set a strong password (minimum 8 characters, uppercase, lowercase, numbers, special characters)
- System shall store passwords using bcryptjs with minimum 12 salt rounds
- System shall complete registration within 5 minutes of initial request
- System shall support registration in French and English languages

FR-1.2: User Login

- System shall authenticate users using email/phone and password
- System shall implement rate limiting (maximum 5 failed attempts per 15 minutes)
- System shall lock account after 5 consecutive failed login attempts for 30 minutes
- System shall generate JWT tokens with 15-minute expiration for access tokens
- System shall generate refresh tokens with 7-day expiration
- System shall log all login attempts for audit purposes
- System shall support biometric authentication (fingerprint/face recognition) on supported devices

FR-1.3: Account Management

- System shall allow users to view and edit profile information
- System shall allow users to change password with current password verification
- System shall allow users to enable/disable two-factor authentication
- System shall allow users to manage linked phone numbers and email addresses
- System shall maintain account activity history
- System shall allow account deactivation with 30-day recovery period

3.1.2 Know Your Customer (KYC) Verification

FR-2.1: KYC Level 1 (Basic)

- System shall collect basic information: full name, date of birth, phone number, email
- System shall verify phone number ownership via OTP
- System shall store KYC Level 1 status in user profile
- System shall allow Level 1 users to perform transactions up to 500,000 FCFA per day
- System shall complete Level 1 verification within 5 minutes

FR-2.2: KYC Level 2 (Intermediate)

- System shall collect government-issued ID information (national ID, passport, or driver's license)
- System shall integrate with third-party KYC provider for document verification
- System shall perform facial recognition to verify ID holder identity
- System shall require proof of address (utility bill or bank statement not older than 3 months)
- System shall store verified documents securely with encryption
- System shall complete Level 2 verification within 24 hours
- System shall allow Level 2 users to perform transactions up to 5,000,000 FCFA per day

FR-2.3: KYC Level 3 (Enhanced)

- System shall collect comprehensive financial information
- System shall require bank reference or employer verification
- System shall perform enhanced due diligence checks
- System shall allow Level 3 users unlimited daily transaction limits
- System shall complete Level 3 verification within 5 business days

FR-2.4: KYC Compliance

- System shall implement BEAC KYC guidelines for financial institutions
- System shall maintain audit trail of all KYC verification attempts
- System shall flag suspicious patterns for manual review
- System shall comply with CRF reporting requirements for high-value transactions (>10,000,000 FCFA)

3.1.3 Virtual Card Provisioning

FR-3.1: Card Creation

- System shall allow users to create virtual cards after KYC Level 1 verification
- System shall generate unique card numbers (16 digits) for each virtual card
- System shall generate CVV (3 digits) and expiration date (valid for 3 years)
- System shall support multiple virtual cards per user (maximum 10 cards)
- System shall assign card names for user identification (e.g., "Online Shopping", "Travel")
- System shall set card spending limits by default (1,000,000 FCFA per day)
- System shall allow users to customize spending limits within KYC tier limits

FR-3.2: Card Management

- System shall display card details securely (last 4 digits visible, full number only on request)
- System shall allow users to activate/deactivate cards

- System shall allow users to freeze/unfreeze cards temporarily
- System shall allow users to delete cards (with transaction history retention)
- System shall support card renewal before expiration
- System shall track card usage statistics and spending patterns

FR-3.3: Card Security

- System shall implement 3D Secure authentication for online transactions
- System shall support dynamic CVV generation for enhanced security
- System shall allow users to set transaction notifications for each card
- System shall implement velocity checks to prevent rapid-fire transactions
- System shall support card blocking for reported loss or theft

3.1.4 Payment Processing

FR-4.1: Transaction Initiation

- System shall accept payment requests from authenticated users
- System shall validate transaction amount against card spending limits
- System shall validate transaction amount against daily/monthly limits
- System shall verify card status (active, not frozen, not expired)
- System shall verify sufficient balance or credit availability
- System shall initiate transaction processing within 2 seconds of user confirmation

FR-4.2: Transaction Processing

- System shall route transactions to appropriate payment gateway based on transaction type
- System shall implement 3D Secure authentication for high-value transactions (>2,000,000 FCFA)
- System shall support both online and offline transaction processing
- System shall implement transaction timeout handling (maximum 30 seconds)
- System shall maintain transaction state throughout processing lifecycle
- System shall implement retry logic for failed transactions (maximum 3 attempts)

FR-4.3: Transaction Settlement

- System shall settle transactions within 24 hours of authorization
- System shall provide settlement reports to merchants
- System shall support both immediate and batch settlement modes
- System shall implement reconciliation between transaction records and settlement reports
- System shall handle partial refunds and chargebacks

FR-4.4: Multi-Currency Support

- System shall support transactions in FCFA (primary currency)

- System shall support transactions in USD and EUR for international payments
- System shall implement real-time currency conversion using market rates
- System shall display conversion rates to users before transaction confirmation
- System shall store transaction amounts in both original and FCFA equivalent

3.1.5 Fraud Detection and Prevention

FR-5.1: Real-Time Fraud Monitoring

- System shall monitor all transactions for fraudulent patterns in real-time
- System shall implement machine learning models for anomaly detection
- System shall flag transactions exceeding user's typical spending patterns
- System shall flag rapid-fire transactions from different geographic locations
- System shall flag transactions outside user's typical transaction hours
- System shall flag transactions with unusual merchant categories

FR-5.2: Fraud Prevention Rules

- System shall implement velocity checks (maximum 5 transactions per minute per card)
- System shall implement geographic velocity checks (transactions from different countries within 1 hour)
- System shall implement amount velocity checks (rapid increase in transaction amounts)
- System shall implement merchant velocity checks (multiple transactions to same merchant within 1 minute)
- System shall block transactions matching known fraud patterns
- System shall implement whitelist/blacklist functionality for merchants

FR-5.3: Fraud Response

- System shall immediately block flagged transactions pending verification
- System shall notify users of blocked transactions via SMS and push notification
- System shall require user confirmation for suspicious transactions
- System shall implement challenge-response authentication for high-risk transactions
- System shall escalate high-risk transactions to manual review team
- System shall maintain fraud incident logs for analysis and reporting

3.1.6 Notifications and Alerts

FR-6.1: Transaction Notifications

- System shall send SMS notification for every transaction within 30 seconds
- System shall send push notification for every transaction within 30 seconds
- System shall include transaction amount, merchant, and timestamp in notifications
- System shall allow users to customize notification preferences per card
- System shall support notification in French and English

FR-6.2: Security Alerts

- System shall send alerts for login attempts from new devices
- System shall send alerts for password change requests
- System shall send alerts for KYC verification status changes
- System shall send alerts for card creation/deletion
- System shall send alerts for suspicious transaction patterns
- System shall send alerts for account lockout events

FR-6.3: Promotional Notifications

- System shall send promotional offers and rewards notifications
- System shall allow users to opt-in/opt-out of promotional communications
- System shall respect user notification preferences
- System shall limit promotional notifications to maximum 2 per week per user

3.1.7 Transaction History and Reporting

FR-7.1: Transaction History

- System shall maintain complete transaction history for all users
- System shall display transactions with amount, merchant, timestamp, and status
- System shall allow filtering by date range, amount, merchant, and status
- System shall allow searching transactions by merchant name or transaction ID
- System shall provide transaction export functionality (CSV, PDF formats)
- System shall retain transaction history for minimum 7 years for regulatory compliance

FR-7.2: Financial Reporting

- System shall generate monthly account statements
- System shall generate spending analysis reports by merchant category
- System shall generate tax-compliant financial reports
- System shall support custom report generation
- System shall allow report scheduling and automated delivery
- System shall maintain audit trail of all report generation and access

3.1.8 Customer Support

FR-8.1: In-App Support

- System shall provide FAQ section with searchable content
- System shall provide in-app chat support during business hours (8 AM - 6 PM CAT)
- System shall allow users to submit support tickets
- System shall track support ticket status and resolution
- System shall provide support in French and English

FR-8.2: Issue Resolution

- System shall provide average support response time of 2 hours
- System shall resolve 80% of issues within 24 hours
- System shall escalate unresolved issues to management team
- System shall provide compensation for service failures exceeding SLA

3.2 Non-Functional Requirements

3.2.1 Performance Requirements

NFR-1.1: Response Time

- Login response time: < 2 seconds (95th percentile)
- Transaction initiation: < 2 seconds (95th percentile)
- Transaction processing: < 30 seconds (99th percentile)
- Card creation: < 5 seconds (95th percentile)
- Dashboard loading: < 3 seconds (95th percentile)
- API response time: < 500 ms (95th percentile)

NFR-1.2: Throughput

- System shall support minimum 10,000 concurrent users
- System shall process minimum 1,000 transactions per second
- System shall handle 100,000+ daily active users
- System shall scale horizontally to support 1,000,000+ users

NFR-1.3: Availability

- System shall maintain 99.9% uptime (maximum 43 minutes downtime per month)
- System shall support zero-downtime deployments
- System shall implement automatic failover for critical components
- System shall maintain backup systems in geographically distributed locations

3.2.2 Security Requirements

NFR-2.1: Data Encryption

- All data in transit shall use TLS 1.2 or higher
- All sensitive data at rest shall use AES-256 encryption
- Database encryption keys shall be stored separately from encrypted data
- Encryption keys shall be rotated annually
- System shall implement end-to-end encryption for sensitive communications

NFR-2.2: Authentication and Authorization

- System shall implement role-based access control (RBAC)
- System shall enforce principle of least privilege

- System shall implement multi-factor authentication for administrative access
- System shall implement session timeout after 30 minutes of inactivity
- System shall implement JWT-based authentication with secure token storage

NFR-2.3: Data Protection

- System shall comply with GDPR principles for data protection
- System shall implement data minimization (collect only necessary data)
- System shall provide data export functionality to users
- System shall provide account deletion functionality with data purging
- System shall implement PCI-DSS compliance for payment card data
- System shall implement secure data disposal procedures

NFR-2.4: Audit and Logging

- System shall log all user activities with timestamp and user identification
- System shall log all administrative actions with detailed change tracking
- System shall log all security events (login attempts, permission changes, etc.)
- System shall maintain immutable audit logs
- System shall retain audit logs for minimum 7 years
- System shall implement log monitoring and alerting for suspicious activities

3.2.3 Scalability Requirements

NFR-3.1: Horizontal Scalability

- System shall support stateless application servers for horizontal scaling
- System shall implement load balancing across multiple servers
- System shall support database replication and sharding
- System shall implement caching layer for improved performance
- System shall support asynchronous processing for long-running operations

NFR-3.2: Data Scalability

- System shall support minimum 100 GB database size
- System shall support data archival for historical data
- System shall implement database indexing for query optimization
- System shall support data partitioning by date or user ID

3.2.4 Reliability Requirements

NFR-4.1: Fault Tolerance

- System shall implement redundancy for all critical components
- System shall support automatic recovery from component failures
- System shall implement circuit breaker pattern for external service calls
- System shall implement graceful degradation when services are unavailable

- System shall maintain data consistency across distributed systems

NFR-4.2: Disaster Recovery

- System shall maintain backup systems in geographically distributed locations
- System shall implement automated backup procedures (minimum daily)
- System shall test disaster recovery procedures quarterly
- System shall maintain Recovery Time Objective (RTO) of 4 hours
- System shall maintain Recovery Point Objective (RPO) of 1 hour

3.2.5 Usability Requirements

NFR-5.1: User Interface

- System shall implement intuitive mobile-first design
- System shall support both portrait and landscape orientations
- System shall implement accessibility features (WCAG 2.1 AA compliance)
- System shall support font size customization
- System shall support high contrast mode for visually impaired users
- System shall provide haptic feedback for user interactions

NFR-5.2: Localization

- System shall support French and English languages
- System shall support local currency (FCFA) formatting
- System shall support local date and time formats
- System shall support local phone number formats
- System shall provide culturally appropriate content and messaging

3.2.6 Maintainability Requirements

NFR-6.1: Code Quality

- System shall maintain code coverage minimum 80% for critical modules
- System shall implement automated testing (unit, integration, end-to-end)
- System shall implement continuous integration/continuous deployment (CI/CD)
- System shall maintain code documentation and architectural diagrams
- System shall implement code review process for all changes

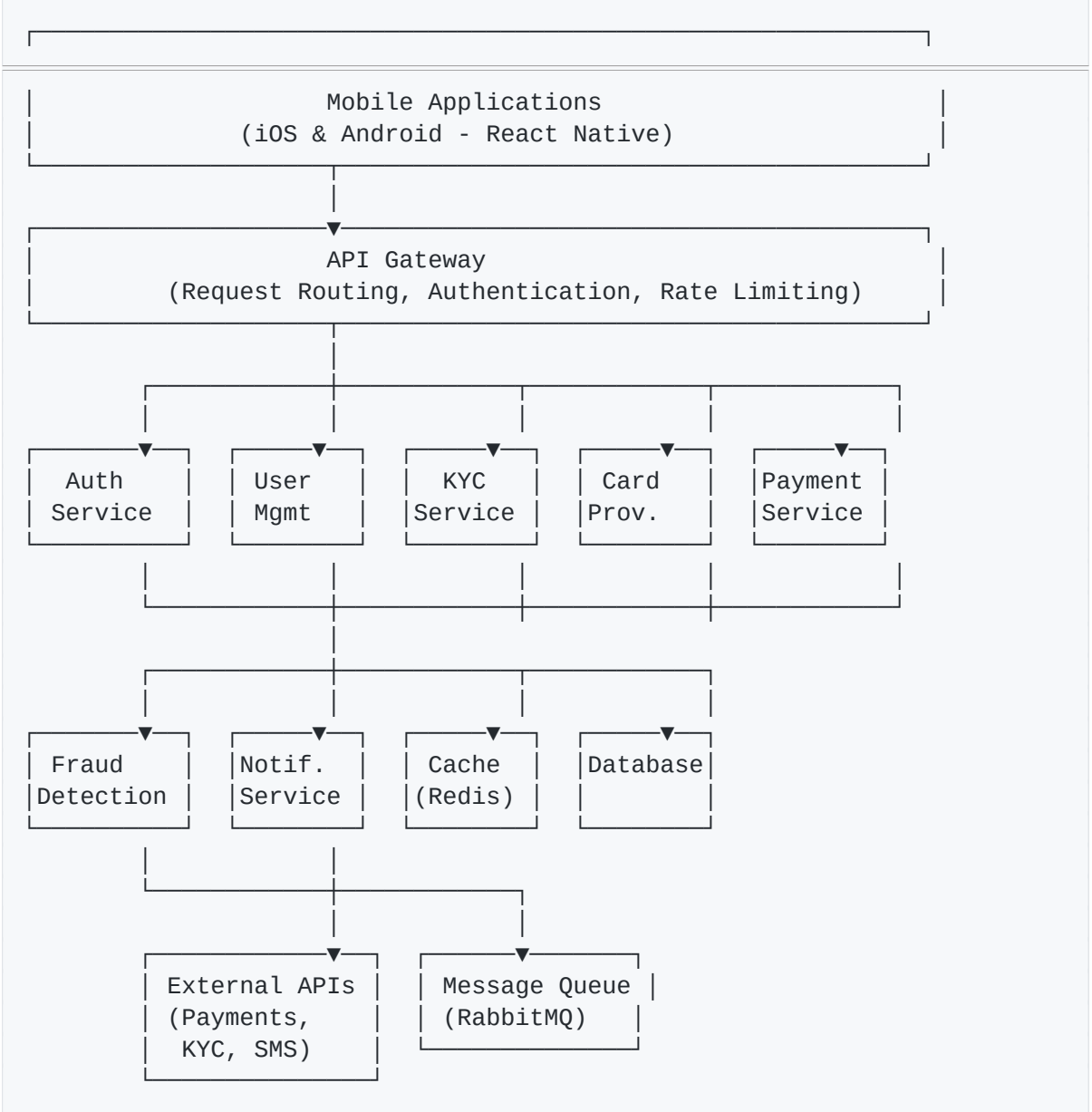
NFR-6.2: System Monitoring

- System shall implement comprehensive system monitoring and alerting
- System shall monitor application performance metrics
- System shall monitor infrastructure resource utilization
- System shall monitor database performance and query optimization
- System shall implement log aggregation and analysis

4. System Architecture

4.1 High-Level Architecture

The Virtual Card Financial System follows a microservices architecture with the following key components:



4.2 Component Descriptions

Mobile Application: Native iOS and Android applications providing user interface for account management, card creation, and transaction processing.

API Gateway: Central routing layer implementing request authentication, rate limiting, and load balancing across backend services.

Authentication Service: Manages user authentication, session management, and JWT token generation.

User Management Service: Handles user profile management, account settings, and user data.

KYC Service: Implements Know Your Customer verification procedures and compliance checks.

Card Provisioning Service: Manages virtual card creation, lifecycle, and integration with card issuance platforms.

Payment Service: Processes transactions, manages payment routing, and handles settlement.

Fraud Detection Service: Monitors transactions for fraudulent patterns using machine learning algorithms.

Notification Service: Delivers SMS and push notifications to users.

Cache Layer: Redis-based caching for session management and performance optimization.

Database: PostgreSQL or MySQL for persistent data storage with encryption.

Message Queue: Asynchronous processing of long-running operations and event distribution.

External APIs: Integration with payment gateways, KYC providers, and SMS services.

5. Regulatory Compliance

5.1 BEAC Compliance

The system shall comply with all applicable BEAC (Banque des États de l'Afrique Centrale) regulations for digital financial services:

5.1.1 Licensing Requirements

- Operator shall obtain necessary licenses from BEAC for financial services provision
- Operator shall maintain minimum capital requirements as specified by BEAC
- Operator shall submit regular compliance reports to BEAC
- Operator shall maintain BEAC-approved governance structure

5.1.2 KYC/AML Compliance

- System shall implement BEAC-compliant KYC procedures for all users
- System shall maintain customer identification records for minimum 7 years
- System shall implement transaction monitoring for suspicious activities
- System shall file Suspicious Activity Reports (SAR) with CRF when required
- System shall implement sanctions screening against international lists

5.1.3 Data Protection

- System shall store customer data within BEAC member states
- System shall implement data protection measures meeting BEAC standards
- System shall maintain data backup and recovery procedures
- System shall implement secure data disposal procedures

5.2 CRF (National Financial Intelligence Unit) Compliance

5.2.1 Reporting Requirements

- System shall report transactions exceeding 10,000,000 FCFA to CRF
- System shall report suspicious transactions within 30 days of detection
- System shall maintain detailed transaction records for CRF reporting
- System shall implement automated reporting to CRF systems

5.2.2 AML/CFT Compliance

- System shall implement anti-money laundering (AML) procedures
- System shall implement counter-terrorism financing (CFT) measures
- System shall screen customers against international sanctions lists
- System shall implement beneficial ownership identification procedures

5.3 Data Protection and Privacy

5.3.1 GDPR Compliance

- System shall comply with GDPR principles for data protection
- System shall implement data minimization principles
- System shall provide data subject rights (access, correction, deletion)
- System shall implement data processing agreements with third parties
- System shall implement privacy by design principles

5.3.2 Local Data Protection Laws

- System shall comply with Cameroon's data protection regulations
- System shall implement appropriate safeguards for personal data
- System shall maintain data protection impact assessments
- System shall implement data breach notification procedures

6. Security Requirements

6.1 Authentication and Authorization

- Multi-factor authentication for sensitive operations
- Role-based access control (RBAC) for administrative functions
- Session management with automatic timeout
- Secure password storage using bcryptjs (minimum 12 salt rounds)
- JWT-based API authentication with secure token storage

6.2 Data Security

- TLS 1.2+ for all data in transit
- AES-256 encryption for sensitive data at rest
- Database encryption with separate key management
- Secure key rotation procedures (annual minimum)
- End-to-end encryption for sensitive communications

6.3 Payment Card Security

- PCI-DSS Level 1 compliance for payment processing
- Tokenization of payment card data
- 3D Secure authentication for online transactions
- Dynamic CVV generation for enhanced security
- Secure card data transmission and storage

6.4 Fraud Prevention

- Real-time transaction monitoring
- Machine learning-based anomaly detection
- Velocity checks and geographic verification
- Whitelist/blacklist functionality
- Automated fraud response procedures

6.5 Audit and Logging

- Comprehensive audit logging of all activities
- Immutable audit logs with tamper detection
- Log retention for minimum 7 years
- Real-time log monitoring and alerting
- Secure log storage and transmission

7. Performance Requirements

7.1 Response Time Targets

Operation	Target (95th Percentile)	Target (99th Percentile)
Login	2 seconds	3 seconds
Card Creation	5 seconds	8 seconds
Transaction Processing	30 seconds	45 seconds
Dashboard Loading	3 seconds	5 seconds
API Response	500 ms	1 second

7.2 Throughput Targets

- Minimum 10,000 concurrent users
- Minimum 1,000 transactions per second
- Support for 100,000+ daily active users
- Scalable to 1,000,000+ users

7.3 Availability Targets

- 99.9% uptime (maximum 43 minutes downtime per month)
- Zero-downtime deployments
- Automatic failover for critical components
- Geographically distributed backup systems

8. Interface Requirements

8.1 User Interface

- Mobile-first responsive design
- Support for portrait and landscape orientations
- Intuitive navigation and user flows
- Accessibility features (WCAG 2.1 AA compliance)
- Customizable font sizes and high contrast mode
- Support for French and English languages

8.2 API Specifications

The system shall provide RESTful APIs with the following endpoints:

Authentication Endpoints

- POST /v1/api/auth/register - User registration
- POST /v1/api/auth/login - User login
- POST /v1/api/auth/refresh - Token refresh
- POST /v1/api/auth/logout - User logout

User Management Endpoints

- GET /v1/api/users/me - Get current user profile
- PUT /v1/api/users/me - Update user profile
- POST /v1/api/users/password/change - Change password
- POST /v1/api/users/2fa/enable - Enable 2FA
- POST /v1/api/users/2fa/disable - Disable 2FA

Card Management Endpoints

- POST /v1/api/cards - Create virtual card
- GET /v1/api/cards - List user's cards
- GET /v1/api/cards/{cardId} - Get card details
- PUT /v1/api/cards/{cardId} - Update card settings
- POST /v1/api/cards/{cardId}/freeze - Freeze card
- POST /v1/api/cards/{cardId}/unfreeze - Unfreeze card
- DELETE /v1/api/cards/{cardId} - Delete card

Transaction Endpoints

- POST /v1/api/transactions - Initiate transaction
- GET /v1/api/transactions - Get transaction history

- GET /v1/api/transactions/{transactionId} - Get transaction details
- POST /v1/api/transactions/{transactionId}/receipt - Get transaction receipt

KYC Endpoints

- GET /v1/api/kyc/status - Get KYC verification status
- POST /v1/api/kyc/level1 - Submit KYC Level 1
- POST /v1/api/kyc/level2 - Submit KYC Level 2
- POST /v1/api/kyc/level3 - Submit KYC Level 3

9. Testing Requirements

9.1 Unit Testing

- Minimum 80% code coverage for critical modules
- Automated unit tests for all business logic
- Test-driven development (TDD) practices
- Continuous integration testing

9.2 Integration Testing

- API integration testing with external services
- Database integration testing
- Payment gateway integration testing
- KYC provider integration testing

9.3 System Testing

- End-to-end user flow testing
- Performance and load testing
- Security penetration testing
- Disaster recovery testing

9.4 User Acceptance Testing

- Testing with representative user groups
- Testing in various network conditions
- Testing on different device types and OS versions
- Accessibility testing with assistive technologies

10. Deployment and Maintenance

10.1 Deployment Environment

- Cloud-based infrastructure (AWS, Google Cloud, or local hosting)
- Containerized deployment using Docker
- Orchestration using Kubernetes
- Infrastructure as Code (IaC) using Terraform or CloudFormation

10.2 Deployment Process

- Automated CI/CD pipeline
- Blue-green deployment strategy for zero-downtime updates
- Automated testing before production deployment
- Rollback procedures for failed deployments
- Deployment approval workflow

10.3 Maintenance and Support

- 24/7 system monitoring and alerting
- Incident response procedures
- Regular security updates and patches
- Database maintenance and optimization
- Log analysis and performance tuning

10.4 Backup and Disaster Recovery

- Automated daily backups
- Geographically distributed backup locations
- Regular disaster recovery testing
- Recovery Time Objective (RTO): 4 hours
- Recovery Point Objective (RPO): 1 hour

11. Appendices

Appendix A: Glossary of Terms

Term	Definition
Virtual Card	Digital payment card created and stored on mobile device
KYC	Know Your Customer - Identity verification process
AML	Anti-Money Laundering - Compliance framework
CFT	Combating the Financing of Terrorism
FCFA	Central African CFA Franc - Cameroon currency
BEAC	Central Bank of Central African States
CRF	National Financial Intelligence Unit (Cameroon)
JWT	JSON Web Token - Authentication token format
OTP	One-Time Password - SMS-based authentication code
3D Secure	Authentication protocol for online card transactions
PCI-DSS	Payment Card Industry Data Security Standard
USSD	Unstructured Supplementary Service Data - SMS banking
GDPR	General Data Protection Regulation - EU data protection law
WCAG	Web Content Accessibility Guidelines
RTO	Recovery Time Objective - Maximum acceptable downtime
RPO	Recovery Point Objective - Maximum acceptable data loss

Appendix B: Regulatory References

The following regulations and standards apply to this system:

11 **BEAC Regulations** - Central Bank guidelines for digital financial services

12 **CRF Requirements** - National Financial Intelligence Unit reporting requirements
13 **Cameroon Data Protection Laws** - Local data protection regulations
14 **GDPR** - General Data Protection Regulation (if processing EU data)
15 **PCI-DSS** - Payment Card Industry Data Security Standard
16 **WCAG 2.1** - Web Content Accessibility Guidelines
17 **ISO 27001** - Information Security Management System Standard

Appendix C: Change Log

Version	Date	Author	Changes
1.0	November 2025	Manus AI	Initial SRS document creation

References

[1] Bank of Cameroon (BEAC) - Guidelines for Digital Financial Services
[2] Cameroon National Financial Intelligence Unit (CRF) - AML/CFT Reporting Requirements
[3] European Commission - GDPR Compliance Guidelines
[4] PCI Security Standards Council - PCI-DSS Standard Version 3.2.1
[5] W3C - Web Content Accessibility Guidelines (WCAG) 2.1
[6] ISO/IEC 27001:2013 - Information Security Management Systems
[7] NIST - Cybersecurity Framework
[8] OWASP - Top 10 Web Application Security Risks

This Software Requirements Specification document is a comprehensive guide for the development of the Virtual Card Financial System tailored for the Cameroon market. All development, testing, and deployment activities should align with the requirements and guidelines specified in this document.