SOFTWARE REQUIREMENTS SPECIFICATION FOR A VIRTUAL CARD PLATFORM

Date: October 26 2025

Prepared by: Kebeh Clovis Bin

1. Introduction

1.1 Purpose

This document presents the software requirements specifications (SRS) for a virtual card platform. It outlines the system's objectives, scope, features, sand performance expectations. The purpose for this specification will be to provide a clear comprehensive reference for developers, testers, and stakeholders throughout the system's life cycle.

The virtual card platform is designed to provide users with a secure and convenient way to create, manage and use virtual payment cards for online and mobile transactions.

1.2 Scope

The virtual card platform will serve as a digital financial service that allows users to:

- Create and manage virtual cards linked to a funding source
- Perform secure online transaction history and generate reports.
- Set spending limits and freeze or deactivate cards at will.
- Receive instant notifications for all card activities
- View detailed transaction history and generate reports.

The solution will include a web and mobile application, and a backend API. It will integrate with external payment gateways and banking APIs to process transactions securely. The system aims to enhance digital payment convenience and user confidence through strong security and real-time visibility into all transactions.

1.3 Acronyms and Abbreviations

Abbreviation	Definition
KYC	Know your Container
API	Application Programming Interface
OPT	One-Time Password

PCI DSS	Payment Card Industry Data Security Standard
JWT	JSON Web Token
UI	User Interface
UX	User Experience

1.4 Overview

The remaining sections describe the system's intended features, user environment, constraints, functional and non-functional requirements, and other related information required for implementation.

2. Overall Description

2.1 Product Perspective

The virtual card platform will operate as an independent application but rely on external banking and payment APIs for transaction processing. It follows modular architecture comprising user-facing applications, backends, services, and third-party integrations.

2.2 Product Functions

Key System functions include

- User account creation, authentication, and KYC verifcation.
- Generation and management of virtual cards.
- Secure payment and authorization and processing.
- Transaction tracking and reporting.
- Customizable spending controls.
- Real-time notifications for all cards activities.
- Administrative control over users and transactions.
- Comprehensive reporting and system analytics.

2.3 Constraints

The constraints include

- ✓ Compliace with PCI DSS and financial regulatory standards.
- ✓ User of HTTPS/TLS 1.3 for all communications.
- ✓ Data must be stored using AES-256 encyption.
- ✓ System limited to approved banking APIs.

3. Specific Requirements

3.1 Functional Requirements.

3.1.1 User Registration and Authentication

I. The system shall allow users to register using email or phone number

II. The system shall verify user identity through a KYC API before account activation.

III. The system shall implement two-factor(2FA) authentication for login and critical actions

IV. The system shall generate and validate JWT tokens for all sessions.

3.1.2 Virtual Card Management

V. The system shall allow users to create and fund new virtual cards.

VI. Users shall be able to freeze, unfreeze, or terminate their virtual cards at any time.

VII. The system shall enable users to set custom spending limits.

VIII. The system shall display card balance, transaction history, and card status in real-time.

3.1.3 Transactions

IX. The system shall authorize and process payments through integrated gateways.

X. The system shall check available balance before approving any transaction.

XI. The system shall record every transaction with timestamp, status, and card reference for security and back-tracking.

XII. The system shall support refunds and chargebacks where merchant APIs allow.

3.1.4 Notifications

XIII. Users shall receive notifications for all successful and failed transactions.

XIV. The system shall alert users when card balance drops below a defined threshold.

XV. The system shall send alerts for any suspicious or unusual activities.

3.1.5 Administration and Reporting

XVI. The admin module shall allow management of users, roles, and permissions.

XVII. The admin shall have access to system usage and performance reports.

XVIII. The admin shall be able to deactivate or restore user accounts.

3.2 Non-Functional Requirements

3.2.1 Scalability and Performance

- The system shall support at least 1,000 concurrent users without performance degradation.

- The transaction processing time shall not exceed 2 seconds under normal load.
- The platform shall support horizontal scaling to handle increased demand.

3.2.2 Security

- All sensitive data shall be encrypted using AES-256.
- All communications must use HTTPS/TLS 1.3.
- Passwords shall be hashed using bcrypt or any other similar algorithm.
- The system shall comply with PCI DSS v4.0 and ISO 27001 standards.
- Users shall be logged out automatically after 10 minutes of in activity.

3.2.3 Usability

- The interface shall be clean, simple, and responsive to different screen sizes.
- The mobile app shall comply with Material Design and iOS UI guidelines.
- Error messages shall be user-friendly and descriptive.

3.2.4 Reliability and Availability

- The system must maintain 99.9% uptime with automatic failover mechanisms.
- Transaction data shall be backed up daily.
- Critical operations must be logged for traceability.

3.2.5 Maintainability

- The architecture shall be modular, separating core services and components.
- Source code shall follow version control using Git.
- APIs shall be documented with Swagger/OpenAPI for ease of integration.

3.2.6 Portability

- The application shall be deployable on Azure, AWS, or Google Clould platform.
- Backend services shall be containerized using Docker.
- The frontend shall run on all major browsers and operating systems.

4 Appendices

4.1 Future Enhancements.

- ✓ Integration with cryptocurrency wallets and blockchain payment systems.
- ✓ AI-based fraud detection for real-time anomaly detection.
- ✓ Support for contactless virtual cards via Apple Pay and Google Pay.