Credit Card Processing

1. Introduction

1.1 Purpose

This document specifies the software requirements for the credit Card Processing System (CCPS) V1.0, a Secure System designed to authorize, process, and settle Credit Card transactions for merchants. This SRS covers the core transaction processing functionalities Including authorization, Capture, refund and settlement. It excludes physical card reader hardware and third-party bank backened Systems.

1.2 Document Conventions

Requirements are labeled, Priorities : High, Medium, Low. Bold for emphasis, italics for notes.

1.3 Intended Audience

Developers : focus on sections 2 and 3
Testers : focus on Section 3
PMs and Marketing : Sections 1 and 2
Suggested reading : 1→ 2→ 3→ 4

1.4 Project Scope

CCPS Supports online/in-person payments, fraud detection, reporting and PCI Compliance Supports Visa, Master Card, and AMEX.

1.5 References:

- PCI DSS v4.0
- ISO 8583:2013
- Internal UI Guide V2.1
- Vision & scope (2024)

2. Overall Description

2.1. Product Perspective

Part of Payment Gateway Suite. Replaces legacy system. Interfaces with POS, payment networks and banks

2.2 Product Functions

Handles authorization, capture, refunds, settlements, fraud detection, and user access control.

2.3 User Classes

- Merchants : moderate skills
- Admins : high technical skills
- Customers : no direct access
- Support : moderate skills

2.4 Operating Environment

Runs on POS terminals, Ubuntu servers, Windows 10/11. Uses PostgreSQL, REST API TLS 1.3.

2.5 Constraints

Must meet PCI DSS v4.0. Use AES-256 encryption. Java backened. React UI. Support ISO 8583

2.6 Documentation

Includes User Manual, API Docs, Tutorials and Troubleshooting Guide.

2.7 Assugmptions & Dependencies.

Needs stable network, third-party fraud Services, bank response times, and identity System integration.

3. Specific Requirments

3.1 Functional Requireiments

- Authorize transactions within 3 seconds
- Capture payments after merchant confirms
- Process merchant-initiated refunds
- Keep transaction logs for 2-years.
- Generate daily settlement reports by 6AM
- Validate card numbers using Luhn algorithm.
- Flag fraud using rule-based checks.
- Support Visa, MasterCard, and AMEX.

3.2 External Interface Requirements

- Use ISO 8583 for payment network messaging
- Provides RESTful APIs for merchants
- ~~EXR~~ Use HTTPS with TLS 1.3 for communication.

3.3 System Features

- Role-based access control.
- Real-time mointoring dashboard
- Automated backup and recovery

3.4 : Non-Functional Requirements.

- 99.9% system availability
- Encrypt all sensitive data.
- Comply with PCI DSS V4.40
- Handle 10,000 transaction /sec.
- UI reponses within 2 seconds.

4. Appendices.

4.1 Glossary

- Authorization : Validates card and funds
- Capture : Finalizes payment
- PCI DSS : Security Standard
- ISO 8583 : Transaction message format

4.2 Future Enhancements

- ~~ML-based fraud detection~~
- ~~Mobile/digital wallets~~
- ~~Multi-currency support~~
- ~~Advanced reporting.~~