Bafna Gold
Date: Page:

Credit Card Processing

1. Introduction

1.1 Purpose

This document specifies the software requirements for the Credit Card Processing (CCPS) v1.0, a secure system designed to authorize, process, and settle credit transactions for merchants. This SRS covers the core transaction processing functionalities including authorisation, capture, refund, and settlement. It excludes physical card reader hardware and third party ~~bank~~ bank backend systems.

1.2 Document Conventions.

Requirement are labeled. Priorities: High, Medium, Low. Bold for emphasis, italic for notes.

1.3 Intended audience.

Developers: focus on Section 2 and 3.
Testers: focus on Section 3.
PMs and Marketing: Section 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 4.0
* 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 systems. 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 environment, Ubuntu Server, Windows 10/11. Uses PostgreSQL, REST APIs, TLS 1.3.

2.5 Constraints.
Must meet PCI DSS v4.0. Use AES-256 encryption. Java backend, ReactUI. Support ISO 8583.

2.6 Documentation
Includes user manual, API docs, Tutorials, and troubleshooting guide.

2.7 Assumptions and dependencies
Needs stable network, third party fraud service, bank response times, and identity system integration.

3. Specification Requirements.
3.1 Functional Requirements.
* 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 6 AM.
* 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.
* Provide RESTful APIs for merchants.
* Use HTTPS with TLS 1.3 for communication.

3.3 System Features.
* Role based access control.
* Real time monitoring dashboard.
* Automated backup and recovery.

3.4 Non-functional requirements.
* 99.9% system availability.
* Encrypt all sensitive data.
* Comply with PCI DSS v4.0
* Handle 10,000 transaction/sec
* UI Responses with 2 seconds.

4. Appendices.
4.1 Glossary
* Authorization validates cards 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.