21/8/25

LAB 2 → SRS Document for Credit Card Processing System.

1. Introduction

1.1 Purpose

The purpose of this document is to specify the functional and non-functional requirements for a credit card processing system (CCPS). The system will handle credit card transactions, authorisations, settlements, fraud detection and reporting for merchants and banks.

1.2 Document conventions

1.2.1 Bold text is used for section titles and important keywords.

1.2.2 Italics are used for emphasis or examples.

1.2.3 Monospace font is used for code, commands and data fields.

1.2.4 Shall indicates mandatory requirements

1.2.5 Should indicates recommended requirements

1.2.6 May indicates optional requirements

1.3 Intended audience and reading suggestions

This document is intended for developers and testers to understand functional and technical requirements. System architects will use it for design and integration details. Project managers and stakeholders can refer to it for a high level system overview and constraints. Bank administrators and merchants will rely on it for operational

workflows and reporting, while auditors will use it for compliance and monitoring.

1.4 Scope

The credit card Processing System (CCPS) enables secure authorisation, processing and settlement of credit card transactions between merchants, banks and customers. It ensures fraud detection, compliance with payment standards and high system availability. The system also provides reporting, dispute management and multi-currency support for seamless financial operations.

1.5 References

1.5.1 PCI-DSS (Payment card Industry Data Security Standard)

1.5.2 ISO 8583 Standard for financial Transaction Messaging

1.5.3 RBI Guidelines for Electronic Payments.

2 Overall Description

2.1 Product Perspective

The Credit Card Processing System is a real-time transaction platform that integrates with merchants, acquirer banks, issuer banks, and card networks. It acts as an intermediary to validate, authorise and process payments. The system supports POS terminals and online platforms. It ensures

Secure communication and compliance with payment standards.

2.2 Product functions

The system authorizes and settles credit card transactions, validates card details, and manages fund transfers. It provides fraud detection mechanisms and ensures secure data handling. It generates reports for merchants and banks. It also supports dispute management and multi-currency transactions.

2.3 User classes and characteristics

2.3.1 Merchants: Initiates and track transactions through POS terminals or online payment portals, view settlement reports and handle customer payment issues.

2.3.2 Cardholders: Use of the system indirectly when making purchases, requiring secure, fast and reliable authorisation of payments.

2.3.3 Bank Staff - Monitor and verify transactions, manage settlements, handle chargebacks and ensure compliance with regulations.

2.3.4 System Administrators: Maintain system availability, manage user roles, monitor security and perform troubleshooting.

2.4 Operation environment

The system will run on secure servers equipped with Hardware Security Modules (HSM) and support merchant POS terminals as well as banking infrastructure. It will operate on Linux or windows servers, use relational databases with encryption, and provide web portals and APIs for integration. Communication will rely on high speed encrypted TCP/IP connections with ISO 8583 messaging. The environment must comply with PCI-DSS standards, use TLS 1.3 for security, and ensure 24/7 availability with 99.99% uptime.

2.5 Design and Implementation constraints

The system must comply with PCI-DSS standards and banking regulations. It must use ISO 8583 messaging for transaction communications. All sensitive data should be encrypted during storage and transmission. The system must support real-time processing with a response time under three seconds. It should run on secure, scalable server infrastructure and ensure compatibility with existing bank and merchant systems.

2.6 User Documentation

The system will provide a user manual for merchants, banks and administrators with step-by-step instructions for operations. online help and FAQs will be available within the web portal. API documentation will be provided for technical teams integrating the system with POS or e-commerce platforms. Training guides and quick reference sheets will be supplied for staff and merchants

2.7 Assumptions and Dependencies

2.7.1 The card networks are always available for transaction routing

2.7.2 Issuer and acquirer banks maintain system uptime and reliable communication channels

2.7.3 Merchants and banks have stable internet connectivity for real-time transaction processing.

2.7.4 Customers enters correct card details during transactions.

2.7.5 The system depends on third-party payment gateways and APIs functioning correctly.

2.7.6 Regulatory and compliance requirements remain unchanged.

2.7.7 Security certifications (SSL/TLS) are renewed and valid at all times.

3.	Specific Requirements
3.1	functional Requirement
3.1.1	The system shall validate card details including number, cvv, expiry and balance before authorisation.
3.1.2	The system shall authorise, capture and settle transactions between merchants, acquirer banks and issuer banks
3.1.3	The system shall provide fraud detection by analysing transaction patterns and flagging suspicious activity.
3.1.4.	The system shall encrypt all sensitive customer and transaction data during transmission and storage
3.1.5	The system shall generate daily, weekly and monthly reports for merchants and banks
3.2	Non Functional Requirements
3.2.1	The system shall process transactions within three seconds
3.2.2	The system shall support at least 5000 transactions per second during peak loads.
3.2.3	The system shall maintain 99.99% uptime for high availability
3.2.4	The system shall comply with PCI-DSS and ISO 27001 security standards.
3.2.5	The system shall scale to handle growing merchant and transaction volumes

3.3 External Interface Requirements

3.3.1 The system shall provide a web-based portal for merchants to view transactions, settlements and reports.

3.3.2 The system shall provide a bank admin portal for monitoring transactions, managing disputes and generating compliance reports.

3.3.3 The system shall support POS terminals for in-store credit card transactions.

3.3.4 The system shall interface with issuer and acquirer banks to validate and settle transactions.

3.3.5 The system shall connect with card networks (Visa, Mastercard, etc) for transaction authorisation and routing.

4 Appendices

4.1 Abbreviations

4.1.1 PCI-DSS - Payment Card Industry Data Security Standard

4.1.2 POS - Point of Sale

4.2 Future enhancements

4.2.1 AI driven fraud detection and risk scoring

4.2.2 Blockchain-based settlement for faster and transparent transactions

4.2.3 Biometric authentication support (fingerprint/ face ID)