2. CREDIT CARD PROCESSING SYSTEM (CCPS)

1. Introduction

1.1. Purpose

The purpose of the CCPS is to design & develop a secure, efficient & user-friendly platform for managing credit card transactions. The system enables customers to perform cashless transactions while ensuring authentication, authorization, fraud detection & accurate billing. The system is intended to serve as the core transaction handler b/w the customer, merchant & bank thereby reducing the risks of fraud & errors that can occur in manual payment systems. It will also enhance transaction speed & provide accurate reporting to all stakeholders.

1.2 Document Conventions

* This document follows IEEE SRS standard structure.
* Double underlining used for main headings & single underlining is used for sub headings.
* Plain text used for detailed explanations.

1.3 Intended Audience

* Customers : Use the system for safe & convenient payments.
* Merchants : Accept payments from customers through online / point of sale systems.
* Bank / Financial Institutions : Manage card data, Billing, settlement & fraud detection.
* Developers : Build & maintain the software.
* Testers : Ensure reliability & security of the system.

1.4 Scope

The CCPS will allow customers to make purchases via credit card in both online & offline environments. The scope includes transaction authorization, validation of customer identity, secure fund transfer, monthly statement generation & fraud prevention measures. The system will support integration with existing banking infrastructure, merchant services, & govt. compliance bodies. The ultimate goal is to provide secure, real time processing of credit card transactions with minimal downtime & max convenience.

1.5 References

* IEEE 830 : Recommended practice for SRS
* RBI Payment gateway guidelines
* PCI DSS security standards.

2. Overall Description

2.1 Product Perspective

The CCPS is a middleware application functioning b/w the bank, customer & merchant. It provides APIs for integration with merchant systems & mobile apps for customers. It acts as an extension of the banking environment & must comply with existing data protection & financial transaction protocols

2.2 Product Functions

* Cardholder authentication : Verifying customer identity using PIN, OTP / Biometric methods.
* Transaction authorization : Ensuring sufficient balance or credit limit before approving a transaction
* Fraud detection : Detecting unusual or suspicious transactions based on transaction history.
* Billing & settlement : Generating monthly statements & facilitating timely settlements b/w customers & merchants.
* Reporting : Providing detailed transaction logs for customers, merchants & bank administrators.

2.3 User classes & Characteristics

- Customer: Typically non technical; requires simple & intuitive interface. Needs reliability & secure use.
- Merchant: Requires quick response, high availability & integration support with existing POS or online store.
- Bank Administrator: Skilled technical staff responsible for monitoring transactions, handling fraud alerts & maintaining records.

2.4 Operating Environment

- Hardware: Standard server infrastructure with redundancy
- Software: Java / Python / .NET backend, MySQL database
- Network: High speed secure internet connection, SSL/TLS for encryption.
- Platform: Web browser, Android/iOS app, POS device.

2.5 User Documentation

The system will be accompanied by

- A customer user manual for cardholders describing the usage
- Merchant guide describing POS setup, integration & troubleshooting
- Bank Administrator Guide including security rules, fraud handling, reporting features.
- Online help documentation & FAQs

2.6 Design & Implementation Constraints

* Must comply with PCI DSS standards for card security
* OTP & two factor authentication are mandatory
* Transactions must complete within 3s
* Must support ACID properties in transaction handling

2.7 Assumptions & Dependencies

Reviewed 19/8/25

* Customer will provide correct card details
* Banking & payment gateway services are always available
* Mobile network & Internet stable.

2.8 Appendix

* OTP – One time password
* PCI DSS - Payment card Industry Data security standard
* RBI – Reserve Bank of India.

3. Specific Requirements

3.1 Functional Requirements

* Authenticate customer using PIN/OTP
* Authorize transactions after checking credit limit
* Generate unique transaction ID
* Maintain records of all transactions
* Provide monthly billing statements.

3.2 Non Functional Requirements

* Must ensure secure transactions using encryption
* Response time within 3s
* System uptime should be 99.9%
* Interface should be user friendly & support mobile/web

3.3 External Interface Requirements

* User Interface: Customer app, Merchant portal, Admin dashboard
* Hardware Interface: POS machines, ATMs, readers
* Software Interface: Bank CBS, payment gateways, SMS/Email services
* Communication Interface: Secure HTTPS, Encrypted API calls

4. System Features

* Authentication Module: Validate user identity with OTP/PIN
* Transaction Processing Module: Handles purchase authorization & settlement
* Fraud Detection Module: Identifies suspicious activities
* Billing Module: Generate monthly statements
* Admin module: Provides reports & monitoring tools.