Bafna Gold
Date: Page:

2) SRS for credit card processing:-

1. Introduction

1.1 Purpose

Purpose of this document is to define requirements for Credit card Processing system (CCPS). It is designed to securely authorize, process and settle credit card transactions between customer merchants & banks. This SRS will serve as a reference to stakeholders to ensure system meets security, reliability and performance expectations.

1.2 Scope

CCPS will handle the complete life cycle of credit card transactions, including authorization, authentication, transaction logging, fraud detection & settlement. Banks and payment network will interact with the system to verify funds & complete settlements. The system aims to reduce transaction errors ensure regulatory compliance and provide high-speed, secure and reliable payment processing.

1.3 Document Conventions

This document follows IEEE 830 standard for SRS. Functional requirements are described in clear, structured paragraphs while non-functional requirements are expressed in plain language by implementing explanation for all technical terms.

1.4 Intended Audience

It includes Software developers, testers, project managers and system architects involved in development of Credit card Processing System. Additionally it is meant for banking officials compliance officers and stakeholders who require an understanding of System's functionality & regulating aspects.

1.5 References

→ IEEE Std 830-1998: IEEE recommended practice for software requirements specifications.
→ PCI DSS compliance standards
→ ISO 8583 standard for financial Transaction Messaging.

2. Overall Description

2.1 Product Perspective

Credit card Processing System will act as an intermediary between merchants, customers, issuing banks, and payment networks. It will integrate with Point of Sale [POS] terminals, online payment, gateways and banking System.

2.2 Product Functions

It will authorize transactions by validating card details, check balances with issuing banks and approve & decline requests. It will log each transaction, detect suspicious activity using fraud detection algorithms and handle settlements between bank & merchants.

2.3 User characteristics

Customers are expected to have minimal technical knowledge and simply use their credit cards for purchases. Merchants will use POS systems or online portals to initiate transactions. Bank administrators and auditors will use back-end tools for monitoring and compliance checks.

2.4 Constraints

System must comply with PCI-DSS standards to protect sensitive cardholder data. It must process transactions within 2-5 seconds and be available 24/7. Strong encryption is mandatory for data transmission.

2.5 Assumptions and Dependencies

The System assumes that customers provide valid card details and that payment networks are available. It also depends on reliable internet connectivity and bank servers for processing requests.

3. Specific Requirements

3.1 Functional Requirements.

→ System must validate card details before processing. It shall also authorize & decline transactions based on available funds & fraud detection checks

→ System shall generate unique Transaction ID for each request.

→ It shall log every transaction in a secure database for auditing.

→ It sends transaction responses back to merchant within 2-5 seconds.

→ System shall provide an API interface for integration with POS terminals and online payment gateways.

→ It shall allow administrators to monitor transactions, generate reports, and review suspicious activities.

3.2 Non-Functional Requirements

Security: System must comply with PCI DSS standards and use AES-256 encryption.

Performance: It must process upto 10,000 concurrent transactions per second.

Reliability: It provide 99.9 uptime & ensure disaster recovery within 1 hour of failure.

Scalability: Support future growth in transaction volume & merchant base.

Usability: Interface must be user-friendly with clear error-message for customers & merchants.

Maintainability: System must allow easy updates without disrupting ongoing operations.

3.3 External Interface Requirements.

System will provide APIs for integration with merchant applications, POS devices, and online payment gateways. It will support HTTPS communication & work with standard databases for transaction logging.

5. Appendices

5.1 Glossary

A Transaction ID is unique identifier generated for each credit card transaction. Authorization is process of verifying card details & funds availability, while Settlement refers to transferring funds from customer accounts to merchant accounts.

5.2 Future Enhancements

Future improvements may include biometric authentication for higher security, AI driven fraud detection systems, blockchain-based settlements for transparency & support for multi-currency international transactions.