19/08/2025

SRS for Credit Card Processing.

1. Introduction :-

1.1 Purpose:

The purpose of this system is to enable secure, efficient and accurate processing of credit card transactions b/w customers, merchants and banks. The system will reduce manual errors, prevent fraud, and maintain financial transaction integrity.

1.2. Document Conventions:-

The term 'shall' indicates mandatory requirements and 'should' indicates desirable but optional features. Functional requirements are simple with shall term. Non-functional are stated with time, accuracy and reliability.

1.3. Intended Audience :-

- Developers - implementation
- Testers - requirement validation
- Staff - usage
- Instructors - project evaluation

1.4 Product Scope :-

It provides end-to-end platform for handling payment requests. It includes transaction authorization, fraud detection, settlement and reposting. Future scalability for mobile wallets and global payment network is also considered.

1.5. References :-

- IEEE SEE standard.
- Visa, MasterCard, and American Express. API integration
- NIST Cybersecurity standards for financial systems.

2. Overall Description

2.1 Product Perspective :-

The system acts as middleware b/w merchants, issuing banks, and acquiring banks.

2.2 User classes and characteristics :-
- Merchant : initiates payment
- customer : provides credit card info
- Bank system : validates and authorize

2.3 Product features :-
- validate credit card entered
- forward the request of bank authorization
- Generate daily transaction reports for auditing

2.4 Operating Environment
- OS : Windows / Linux
- Database : MySQL
- Secure communication via HTTPS

2.5 Design and implementation constraints :-
- Compliance with PCI DSS standards.
- Secure data transmission
- Real time transaction complete 2-3 sec
- High system availability.

3 System Features :-
3.1 Functional requirements :-
- shall validate card details entered.
- shall request authorization from bank.
- shall notify merchants of transaction success or failure
- shall generate reports.

3.2 Non-Functional requirements :-
- shall ensure 99.9% uptime.
- shall support transaction loads
- shall provide response times of under 3sec.
- shall log all activities for security

3.2 Domain requirements.
- must comply with financial regulations

- must integrate with existing gateways.
- must support multiple currencies.
- must maintain transaction

3.4. External Requirements:-
- User interface - web & mobile platform
- Hardware, Software, Communication interface.
- Banking interface - real time communication

A. Appendix:-
A.1. Acronyms:-
- PCI DSS - Payment card industry data security standard.
- CVV - Card verification value

4.2. Glossary:-
- Authorization - Approval of a transaction by bank
- Fraud detection: identify suspicious.
- encryption: securing sensitive data.