SatyamPay Payment Gateway – Complete Documentation

1. Introduction

This platform is a secure online payment gateway that allows businesses to pay in and pay out through UPI.

Objectives of SatyamPay:

2. Accept online payments
3. Provide real-time transaction updates
4. Offer merchant dashboard
5. Provide pay in and pay-out
6. Ensure regulatory compliance

Stakeholders :

1. Merchant
2. Customer
3. Bank

Payment Flow :

Step-by-Step Flow

1. Merchant calls Create Order API
2. Gateway generates Order ID
3. Customer completes payment
4. Bank authorizes payment
5. Gateway verifies signature
6. Webhook sent to merchant
7. Settlement process starts

Customer → Merchant → Gateway → Bank → Gateway → Merchant

System Architecture Overview

System Architecture defines:

- The structural components of the platform
- How these components interact with each other
- How payment data flows securely through the system

SatyamPay is designed as a scalable, modular, and secure B2B payment processing platform capable of handling high-volume financial transactions with regulatory compliance.

1. High-Level Payment Flow

The standard transaction lifecycle is as follows:

Customer
→ Merchant Website / Application
→ SatyamPay API Gateway
→ Payment Processing Engine
→ Bank / NPCI / Card Network
→ SatyamPay Settlement Engine
→ Merchant Bank Account

This architecture ensures secure transaction routing, real-time status updates, fraud detection, and regulated settlement processing.

2. Core System Components

The SatyamPay architecture is divided into the following primary layers:

1. API Gateway Layer
2. Authentication & Authorization Service
3. Payment Processing Engine
4. Database Layer
5. Webhook Service
6. Merchant Dashboard
7. Admin Panel

Each component is logically separated to ensure scalability, security, and maintainability.

API Gateway Layer

The API Gateway acts as the entry point for all external requests from merchants.

Responsibilities:

- Receive all API requests
- Validate API format and structure

Authentication & Authorization Service

This layer ensures that only authorized merchants can access the platform.

1. Validate Merchant ID
2. Verify API Key
3. Validate request signature (HMAC SHA256)
4. Generate and verify JWT tokens
5. Enforce role-based access control (RBAC)

If authentication fails, the request is rejected immediately with an appropriate error response.

Payment Processing Engine :

The Payment Processing Engine is the core transaction management system.

Responsibilities:

- Create payment orders
- Persist transaction records
- Validate transaction parameters
- Route transactions to appropriate banking channel
- Process bank responses
- Update transaction status
- Trigger webhook notifications

Transaction Flow Example:

1. Merchant submits payment creation request
2. Order is generated and stored
3. Customer completes payment
4. Bank returns authorization response
5. System verifies signature
6. Transaction status updated
7. Webhook triggered

Webhook Service

The Webhook Service enables real-time communication between SatyamPay and the merchant system.

Functionality:

- Send transaction updates automatically

- Sign webhook payload using secret key
- Retry delivery on failure (up to defined limit)
- Maintain delivery logs
- Support idempotency to prevent duplication

Example Webhook Payload:

```
{
"event": "payment.success",
"order_id": "123",
"amount": 1000
}
```

This ensures merchants do not need to poll APIs repeatedly.

Merchant Dashboard

The Merchant Dashboard is a secure web interface provided to merchants.

Features:

- Real-time transaction monitoring
- Refund initiation
- Revenue analytics
- API usage logs
- Webhook logs
- Payout management
- User access control

The dashboard operates as a separate service layer interacting with backend APIs.

Admin Panel

The Admin Panel is used internally by SatyamPay operations and compliance teams.

Functionalities:

- Merchant onboarding approval
- Fraud analysis
- Settlement adjustments
- Manual refunds
- management

Access is restricted using role-based permissions.

Security Architecture Layers

SatyamPay follows a multi-layer security model:

Layer 1 – HTTPS Encryption
Layer 2 – API Authentication
Layer 3 – Signature Validation
Layer 4 – Fraud Detection Controls
Layer 5 – Database Encryption
Layer 6 – Role-Based Access Control

This layered security ensures regulatory compliance and transaction integrity.