Software Design Document (SDD) – Sample

1.Introduction

This Software Design Document (SDD) describes the architectural and detailed design of the **Passport Automation System (PAS)**. It translates the requirements specified in the Software Requirements Specification (SRS) into a structured technical design that can be used by developers, testers, and maintenance teams.

2.System Architecture

The Passport Automation System follows a **layered (multi-tier) architecture** to ensure scalability, security, and maintainability.

2.1 Architecture Overview

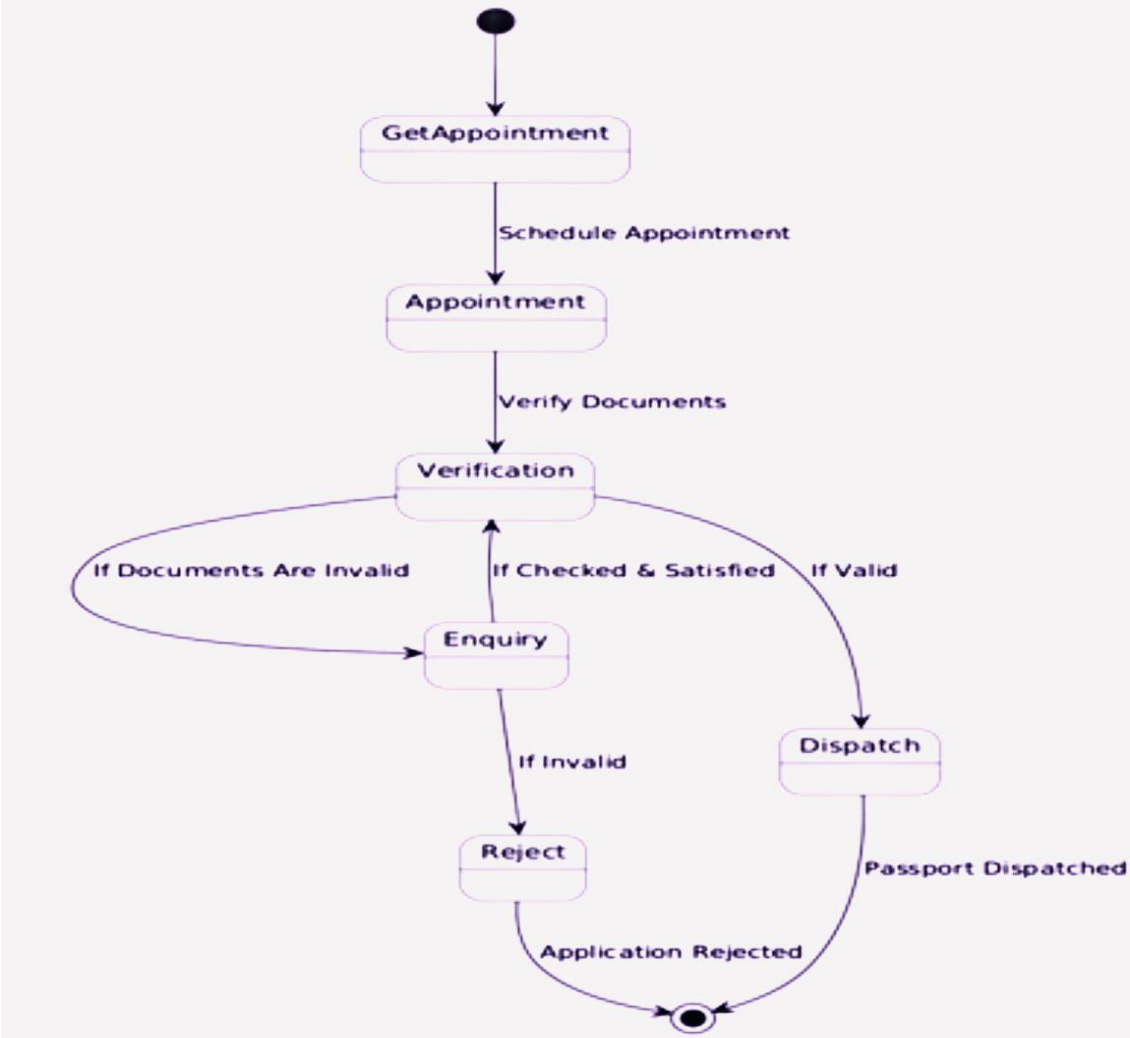
The system is divided into the following layers:

- **Presentation Layer**: Web-based user interface for Applicants, Administrators, and Police Authorities.
- **Business Logic Layer**: Handles application processing, validation, verification workflow, and decision-making logic.
- **Data Layer**: Manages data storage, retrieval, and consistency using a relational database.
- **Integration Layer**: Connects external services such as payment gateways, email/SMS notifications, and police verification systems.

2.2 Major Modules

- User Registration & Authentication Module
- Passport Application Management Module
- Appointment Scheduling Module
- Payment Processing Module
- Verification & Approval Module
- Status Tracking & Notification Module
- Administrative & Reporting Module

3.Detailed Design



3.a Flow Chart Diagram for Passport Automation System

3.b Class Diagram

4.Database Design

4.1 Entity Relationship Description

Main entities include:

- Applicant
- Application
- Document
- Verification
- Payment

- Passport

Relationships:

- One Applicant can submit many Applications.
- Each Application has one Payment and one Verification record.
- Each approved Application generates one Passport.

4.2 Data Storage Approach

- Relational Database Management System (RDBMS)
- Normalized tables to reduce redundancy
- Encrypted storage for sensitive fields (passwords, IDs)
- Regular backups and recovery mechanisms

5.Design Constraints

5.1 Hardware Constraints

- Requires internet-enabled devices (desktop/laptop/mobile)
- Server infrastructure must support concurrent users

5.2 Software Constraints

- Web browser compatibility (Chrome, Firefox, Edge)
- Dependence on third-party payment and notification services

5.3 Regulatory Constraints

- Compliance with government data protection and privacy laws
- Secure handling of national identity information