Passport Automation System

1. Introduction

1.1 Purpose

The purpose of this document is to clearly define the requirement for the Passport automation system (PAS). The system aims to simplify & automate the process of passport application, verification, issuance & renewal for citizens. The SRS will guide developers, testers & users by providing a comprehensive understanding of the system's functionalities, constraints & performance requirements

1.2 Scope of the Document

This system will facilitate online passport application, document verification, appointment scheduling & tracking of application status. It will also generate reports & manage user profiles. The system is intended to improve efficiency, reduce paperwork, & enhance transparency in passport issuance procedures. The system will be accessible to applicants & govt. officials through web & mobile platforms.

1.3 Overview

The passport automation system will streamline the entire passport lifecycle by providing online forms, document uploads, fee payments, appointment booking & status tracking. It will allow govt. officials to verify applicant data, process approvals & manage renewals efficiently. The system will include secure authentication, data encryption & audit trails for accountability

2. General Description

The PAS is designed for two primary users- citizens applying for passports & government officials processing the applications. It will provide interfaces for online registration, application submission, appointment scheduling & status updates. The system will integrate with govt. databases to verify identities & cross check documents. It will ensure high availability, data security & real time processing.

This system will provide notifications via SMS & email for appointment schedules, document requirements & application status. It will be compatible with standard desktop & mobile devices ensuring ease of access. The backend will include secure databases with encryption, automated workflows & reporting tools.

3. Functional Requirements

3.1 User Registration & Login

* Applicants must be able to register with personal information & create a secure login
* Officials must have secure administrative access for verification & approval processes

3.2 Passport Application Process

* Applicants must fill in online form with personal details, upload required documents & submit applications.
* The system must allow applications to track their application status & receive notifications

3.3 Appointment Scheduling

* The system will allow applicants to book slots for document submission & biometric verification

3.4 Document verification

* Government officials can view submitted documents, cross check data and approve or reject applications

3.5 Payment Module

* Applicants should be able to pay application & processing fees through secure payment gateways

3.6 Report Generation

* Officials can generate reports for pending applications, issued passports & renewals.

4. Interface Requirements

4.1 User Interface

* Web-based & mobile friendly interface with easy navigation
* Form validation & step by step instructions for applicants
* Dashboard for officials to view & manage applications

4.2 Integration Interfaces

* Integration with national ID databases (like Aadhaar)
* Integration with payment gateways for online transactions
* Integration with email/sms services for communication

5. Performance Requirements

5.1 Response Time

The system should load pages within 2s & process user requests within 3s under normal load.

5.2 Scalability

The system should handle upto 10,000 simultaneous users during peak hours

5.3 Data Integrity

All users information, documents & payment data must be securely stored & protected against unauthorized access.

6. Design Constraints

6.1 Hardware Constraints

Compatible with standard desktop computers, mobile & biometric scanners

6.2 Software Constraints

* Uses relational DBS like MySQL or PostgreSQL
* Developed using secure frameworks such as Java Spring Boot or Python Django.
* Must comply with govt. IT policies & data protection laws

7. Non Functional Attributes

7.1 Security : Multifactor authentication, encryption of sensitive data & secure session management must be enforced

7.2 Reliability : Backup systems & disaster recovery plans should ensure 99.9% uptime.

7.3 Usability : The Interface must be intuitive, accessible & multilingual for wide adoption

7.4 Portability : Should support major browsers & operating systems without compatibility issues.

7.5 Maintainability : The system must be modular & easily upgradable to accomodate policy changes.

8. Preliminary Schedule and Budget

The system is expected to be completed in 6-7 months. The estimated cost is 12 lakhs covering development & maintenance. It includes software setup, infrastructure & licensing. This will ensure a secure & efficient passport service within the planned timeframe.