5) Passport automation system

* problem statement:
To develop a automated system that streamlines passport application processing, reduces manual errors & accelerates issuance while ensuring data security & compliance

SRS document
Introduction

* purpose of the document:
To specify detailed requirements & system design for the passport automation system to ensure all stakeholder needs are met & guide the development process

* scope of the document:
covers passport application submission, document verification, appointment scheduling, biometric data capture, status tracking & passport issuance

* Overview:
The system automate the entire passport lifecycle from application intake to delivery, providing interfaces for applicants, verification officers & administrators

* General description:
→ Enables online application submission with document upload
→ Supports biometric data collection
→ Automated appointment booking & notification system
→ verification workflows with approval/rejection processing

→ Status tracking & alert notifications for applicants
→ Report generations for administrative use

* Functional requirements
  → User registration & secure login
  → Application form filling with validation & document upload
  → scheduling & managing biometric / verification appointments
  → verification & approval/rejection of applications by officers
  → Issuance & dispatch tracking of passports
  → Notification system for status updats via email / SMS
  → Administrative reporting on applications & processing times

* Interface requirements
  → Responsive web interface accessible on desktops & mobiles
  → Secure document upload functionality
  → Integration with biometric hardware
  → APIs for government database & postal servies
  → Secure https communication for all data transfers

* Performance requirements:
  → Support at least 5000 concurrent users during peak times
  → Process & verify applications within 45 hours on average
  → Real time status updates & notifications
  → System uptime of 99.9% excluding maintenance

* Design constraints
  → must comply with government security & privacy regulations
  → Use encrypted storage for sensitive applicant data
  → Support integration with national ID database
  → System should be modular for future updates
  → Hardware compatability for biometric devices

* Non functional requirements
  → High security & confidentiality of personal data
  → User friendly interface with multi language support
  → Scalable architecture to handle growing application volumes
  → Reliable backup & disaster recovery processes
  → Maintainability with clear documentation

* Preliminary schedule & budget
  → Requirement analysis - 3 weeks
  → System design - 4 weeks
  → Development - 12 weeks
  → Testing - 4 weeks
  → Deployment - 2 weeks
  → Budget estimation = 35-40 lakhs