Software Requirements Specification (SRS)
(IEEE 830-Style Format)

1. Introduction

This document follows an IEEE-style Software Requirements Specification (SRS) structure. It defines the purpose, scope, terminology, references, and system overview for Passport Automation System.

1.1 Purpose

If the entire process of 'Issue of Passport' is done manually, then it would take several months for the passport to reach the applicant. Because the number of passport applicants is increasing every year, an Automated System becomes essential to meet the demand. So, this system uses several programming and databases to elucidate the work involved in this process. As this is a matter of Nation, system has been carefully verified and validated in order to satisfy it.

1.2 Document Conventions

This document uses IEEE-style numbering, requirement identifiers (FR-#, NFR-#), and standard terminology conventions.

1.3 Intended Audience and Reading Suggestions

This document is intended for the following audiences involved in the Passport Automation System:

- Project sponsors and stakeholders – to understand the system objectives, scope, and overall requirements.
- Software engineers and designers – to analyze functional and non-functional requirements and design the system architecture accordingly.
- Test engineers – to derive test cases for verification, validation, and quality assurance.
- Deployment and maintenance teams – to understand system configuration, operational environment, and maintenance requirements.

Reading Suggestions:

- Readers are encouraged to review the sections of this document that are most relevant to their role and responsibilities. This approach enables efficient understanding and effective use of the specification

1.4 Project Scope

The System provides an online interface to the user where they can fill in their personal details

- The authority concerned with the issue of passport can use this system to reduce his workload and process the application in a speedy manner.
- Provide a communication platform between the applicant and the administrator.
- Transfer of data between the Passport Issuing Authority and the Local Police for verification of applicant's information.

1.5 References

[1] **IEEE Std 830-1998**, *IEEE Recommended Practice for Software Requirements Specifications*, IEEE Computer Society, 1998.

[2] **IEEE Std 1016-2009**, *IEEE Standard for Information Technology – Systems Design – Software Design Descriptions*, IEEE Computer Society, 2009.

[3] **Pressman, R. S.**, *Software Engineering: A Practitioner's Approach*, McGraw-Hill Education, 7th Edition.

2. Overall Description.

2.1 Product Perspective

The PAS acts as an interface between the 'applicant' and the 'administrator'. This system tries to make the interface as simple as possible and at the same time not risking the security of data stored in. This minimizes the time duration in which the user receives the passport.

2.2 Product Functions

Major system functions include:

- Secure Registration of information by the Applicants.
- Message box for Passport Application Status Display by the Administrator.
- Administrator can generate reports from the information and is the only authorized personnel to add the eligible application information to the database

2.3 User Classes and Characteristics

- Applicant - They are the people who desire to obtain the passport information to the database.
- Administrator - He has the certain privileges to add the passport issue of passport. He may contain a group of persons under him to v give suggestion whether or not to approve the dispatch of passport.
- Police - He is the person who upon receiving intimation from the PA verification of the applicant and see if he has any criminal case against him before or at present. He has been vetoed with the power to decline an application by suggesting it to the Administrator if he finds any discrepancy with the applicant. He communicates via this PAS.
- Database administrator: Admin can update, delete, modify the detail of the applicants which are filled by them only of their respective department.

2.4 Operating Environment

The Passport Automation System is designed to operate in a modern, scalable, and secure computing environment. The operating environment details are as follows:

- The system shall provide a web browser–based interface, allowing users to access the application using standard browsers such as Chrome, Firefox, or Edge.
- The system shall support a mobile-responsive design, enabling seamless access from desktops, laptops, tablets, and smartphones.
- The backend of the system shall be cloud-hosted, ensuring high availability, scalability, and reliability.
- The system shall use a relational database to store applicant details, application records, verification data, and passport information.
- The operating environment shall support secure internet connectivity for communication between clients and servers.
- The system shall be compatible with commonly used operating systems such as Windows and Linux.

2.5 Design and Implementation Constraints

- The applicants require a computer to submit their information.
- Although the security is given high importance, there is always a chance of intrusion in the web world which requires constant monitoring.
- The user has to be careful while submitting the information. Much care is required.

2.6 User Documentation

User manuals, onboarding guides, and helpdesk support documents will accompany the release.

2.7 Assumptions and Dependencies

- The Applicants and Administrator must have basic knowledge of computers and English Language.
- The applicants may be required to scan the documents and send.

3. System Features (Functional Requirements)

3.1 User Registration & Login

FR1: The system shall allow users to register with unique credentials (email/phone).

FR2: The system shall allow users to log in and log out securely.

FR3: The system shall provide a forgot password / reset password feature.

3.2 Application Management

FR4: The system shall allow users to apply for a new passport or renew an existing one.

FR5: The system shall allow users to fill in and submit an online application form.

FR6: The system shall enable users to upload required documents (ID proof, address proof, photo).

3.3 Appointment & Scheduling

FR7: The system shall allow users to book an appointment at a Passport Seva Centre.

FR8: The system shall allow users to reschedule or cancel appointments.

3.4 Payment Processing

FR9: The system shall allow users to pay application fees online via integrated payment methods.

FR10: The system shall generate payment receipts and update status in real time.

3.5 Verification & Validation

FR11: The system shall forward user application details to verification authorities (employee / admin / police).

FR12: The system shall allow authorized users to update verification status (approved/rejected/hold).

FR13: The system shall notify the user of verification updates.

3.6 Status Tracking

FR14: The system shall allow users to track real-time status of applications (submitted → verified → processed → issued).

FR15: The system shall send email/SMS notifications at each major stage.

3.7 Passport Issuance

FR16: The system shall generate the approval for passport issuance once all checks are complete.

FR17: The system shall allow administrators to manage printing and dispatch of passports.

FR18: The system shall update delivery tracking information for users.

3.8 Administrative Functions

FR19: The system shall provide role-based access (Admin, Verifier, Police Officer).

FR20: The system shall allow admins to generate reports and view system logs.

4. External Interface Requirements

4.1 User Interfaces

The system shall provide a web-based graphical user interface (GUI) for applicants, administrators, and verification authorities.
The user interface shall allow applicants to:

- Register and log in

- Fill passport application forms
- Upload required documents
- View application status

The administrator interface shall allow:

- Viewing and verifying applications
- Approving or rejecting applications
- Issuing passports
- The interface shall be user-friendly, simple, and menu-driven.
- Error messages and system alerts shall be displayed clearly to users.
- The interface shall be accessible through standard web browsers.

4.2 Hardware Interfaces

The system shall operate on standard client-server architecture.
Client side requires:

- Desktop or laptop computer
- Keyboard and mouse
- Internet connectivity

Server side requires:

- Application server
- Database server
- Optional hardware devices:
- Printers for passport printing
- Biometric devices (for future enhancements)
- No specialized hardware is mandatory for basic system operation.

4.3 Software Interfaces

The system shall interface with:

- Database Management System (e.g., MySQL) for storing applicant and passport data
- Web server to host the application

The system shall be compatible with:

- Operating systems such as Windows or Linux
- Web browsers like Chrome, Firefox, or Edge

The system may interface with:

- Payment gateway software (if online payment is enabled)
- Email/SMS services for notifications
- The system shall use standard programming languages and frameworks for development.

4.4 Communication Interfaces

The system shall use HTTP/HTTPS protocols for communication between client and server.

Secure communication shall be ensured using encryption (HTTPS).

The system shall support communication between:

- Applicant and system
- Administrator and police verification authority
- The system shall transmit data over the internet.

Notification messages may be sent via:

- Email
- SMS gateways
- Data exchange shall follow standard web communication formats.

5. Non-Functional Requirements

5.1 Performance

NFR1: The system shall support at least 5,000 concurrent users without performance degradation.

NFR2: The system shall load major pages (form, status) within 2–3 seconds under normal conditions.

NFR3: Payment processing shall occur in real time.

5.2 Security

NFR4: The system shall use HTTPS encryption for secure communication.

NFR5: Sensitive user data (passwords, IDs, payments) shall be encrypted in storage.

NFR6: The system shall enforce role-based access control.

NFR7: The system shall defend against common web attacks (SQL injection, XSS).

5.3 Availability & Reliability

NFR8: The system shall provide 99.9% uptime (excluding maintenance).

NFR9: The system shall have automatic backups and recovery plans.

NFR10: The system shall notify users in advance of scheduled downtime.

5.4 Scalability

NFR11: The system shall be scalable to support future growth in users and transactions.

NFR12: The system shall support expansion to integrate biometric modules or additional verification APIs.

5.5 Usability

NFR13: The system shall support a user-friendly interface for all user roles.

NFR14: The system shall support multiple languages.

NFR15: The system shall be accessible for users with disabilities.

5.6 Maintainability

NFR16: The system shall have modular design for easier updates.

NFR17: The system shall maintain clear documentation for developers.

6. System Architecture Overview

The solution follows a layered architecture consisting of:

6.1 Presentation Layer

Provides the user interface for applicants, administrators, and verification authorities.

Handles user interactions such as login, form submission, document upload, and status viewing.

Implemented using web technologies and accessed via standard web browsers.

6.2 Business Logic Layer

Contains the core application logic.

Validates user inputs and application data.

Manages workflows such as application processing, verification, approval, and rejection.

Enforces business rules and decision-making processes.

6.3 Data Layer

Responsible for data storage and retrieval.

Stores applicant details, verification records, passport information, and system logs.

Ensures data consistency, integrity, and security.

6.4 Integration Layer

Facilitates communication with external systems and services.

Handles integration with payment gateways, email/SMS notification services, and verification authorities.

Enables future integration with biometric or government identity systems.

7. System and Data Models (Placeholder)

UML Diagrams

Use Case Diagrams

Class Diagrams

Sequence Diagrams

ER (Entity-Relationship) Diagrams

Applicant

Application

Verification

Passport

Workflow Diagrams

Passport application process

Verification and approval flow

8. Validation and Acceptance Criteria

The Passport Automation System shall be validated to ensure that it meets all specified requirements.

All functional and non-functional requirements must be verified using defined test cases.

Unit testing, integration testing, system testing, and security testing shall be performed.

User Acceptance Testing (UAT) must be successfully completed and approved by authorized stakeholders.

The system shall pass performance and security testing before deployment.

Deployment shall proceed only after all acceptance criteria are met.

9. Appendices

Appendix-A: Glossary

- Applicant – A user applying for a passport.
- Administrator – Authorized personnel managing passport processing.
- Verification Authority – Officials responsible for validating applicant details.
- UAT – User Acceptance Testing.

Appendix-B: Sample Data

- Sample applicant profiles
- Sample application forms
- Sample verification status records
- Sample passport issuance records

Appendix-C: Compliance Checklist

- Data security and privacy compliance
- Government and regulatory standards adherence
- Audit and logging compliance
- Accessibility and usability standards compliance