SRS for a Passport Automation System

1 ~~Introduction~~ INTRODUCTION

1.1 Purpose

The purpose of this document is to define the functio and non-functional requirements for the Passport Automation System (PAS). This system is designed to streamline and automate the entire lifecycle of a passport application, from online Submission to final issuance. This SRS serves as a comprehensive blueprint for the development team and all stakeholders, ensuring a shared understanding of the project's scope and objectives.

1.2 Scope

This SRS addresses the core functionalities of the PAS, including online application submission, secure document uploading, appointment scheduling, and application status tracking. It also covers the internal back-end processes for document verification, application approval, and reporting. The scope does not include the physical manufacturing of passport booklets or their delivery logistics.

1.3 Overview

The PAS will be a secure, ~~be~~ web-based platform accessible to citizens and government staff It will provide a centralized, digital solution to replace manual, paper-based processes, thereby reducing processing times, enhancing data accuracy, and improving the overall user experience for applicants.

2 GENERAL DESCRIPTION

The PAS is intended for use by three primary user classes: Applicants, Processing staff and System administrators. Applicants will utilize a public-facing portal to submit and track their applications. Processing staff at passport centers will use a secure internal dashboard to review and manage applications. System Administrators will have a higher level of access for system configuration user management, and performance monitoring. The system will operate within a highly secure, private cloud environment.

3. FUNCTIONAL REQUIREMENTS

The system shall perform the following core functions:

- Online Application : Provide a secure, dynamic web form for applications to submit new passport applications, renewals, or other related services. The form shall include real-time data validation to ensure accuracy.

- Document Management : Allow applicants to securely upload required digital copies of supporting documents. The system must support various file types and ensure data integrity.

- Appointment scheduling : Enable applicants to book an appointment at a designated passport center for biometric data collection and physical document verification

- Application tracking: Provide applicants with a unique tracking ID to monitor the real-time status of their application throughout the entire process.

- Internal Processing Dashboard: Provide Processing staff with a secure back-end dashboard to review submitted applications, verify documents, and approve or reject applications.

- Payment Integration: Integrate with a secure, government-approved payment gateway to process application fees

- Reporting: Generate comprehensive reports for administrators on application volumes, processing times, and success rates.

4. INTERFACE REQUIREMENTS

- User Interface: The system shall features a responsive, public-facing web portal for applicants and a seperate, role-based internal dashboard staff. Both interfaces must be inuitive and easy to navigate.

- Hardware Interface: The system must be able to interface with standard biometric and document scanners at passport centers for the capture of fingerprints, photographs and physical document data.

- Software Interface. The system shall include an API for potential future integration with other government databases with for identity verification and background checks. All external communication shall be secure

5. PERFORMANCE REQUIREMENTS

- Response time: All page loads and form submissions for applicants shall complete with 3 seconds. Internal staff queries shall return results within 2 seconds.

- Concurrency: The system shall be capable of handling a minimum of 500 concurrent applicants during peak hours without performance degradation.

- Availability: The PAS must maintain an uptime of 99.9% to ensure continuous service to citizens.

6. DESIGN CONSTRAINTS

- Security Compilance: The system must strictly adhere to national security protocols for handling citizen data and sensitive personal information.

- Technology stack: The system shall be developed using a robust and scalable technology stack capable of handling high-traffic and sensitive data with a preference for secure, open-source solutions where applicable.

- Scalability : The architecture must be designed to accomodate a national userbase and a significant increase in applicat modelling.

7. NON-FUNCTIONAL REQUIREMENTS

- Security : The system shall implement end-to-end encryption for all data in transit and at rest. Access to all internal data must be governed by strict role-based access control and multi-factor authentication

- Usability : The applicant portal must be accessible to users with varying level of technical proficiency. The staff dashboard must be streamlined for efficient data processing.

- Reliability : The system must have a robust error handling and logging mechanism, along with a daily data backup and disaster recovery plan.

- Maintainability : The system's codebase must be modular well-documented, and easily adaptable to changes in government policy or regulations.

C. PRELIMINARY SCHEDULE AND BUDGET

- Schedule: The estimated development timeline for a functional core system is 12-18 months, with a additional 6 months for security audits and a phased deployment

- Budget: The preliminary budget for development, based on a specialized team of 6-8 engineerings and security experts, is estimated to be in the range of $500,000, to $800,000. This encludes hardware, infrastructure, and ongoing operational costs.