22/8/25 Date __/__/____

Saathi

④ Passport Authentication System

1. Introduction

1.1 Purpose : The purpose of this document is to define software requirements for a Passport Authentication System. It will provide applicants, administrators and verification authorities with a secure, user friendly platform.

1.2 Scope of this document : This document defines the overall working and main objectives of the Passport Authentication System. It includes a description of the development cost and time required for the project.

1.3 Overview : The Passport Authentication System will centralize all passport-related service, integrating document submission, verification. The system will be accessible nationwide, ensuring efficiency and reducing physical visits to passport offices.

2. General description

The Passport Authentication System will cater to the needs of applicants, passport officials, administrators, verification offices providing a centralized government portal with optional integration into national ID and police verification databases.

3. Functional Requirements

3.1 Application Management

- User registration & authentication
- Document upload & fee payment via payment gateway

Page No. 11

Date ___/___/_____

3.2 Verification & Approval
- Integration with police verification system
- Document validation by authorized officials
- Approval or rejection of applications with reasons

3.3 Tracking & Issuance
- Real-time tracking of application status by applicants
- Notification via email for each stage.
- ~~Status~~ Online grievance redressal & customer support

4. Interface requirements.

4.1 User Interface
- Applicants: Online registration, application forms, payment and tracking.
- Officials: Applications dashboard, verification tools, approval panels.
- Admins: Manage users, monitor system logs, handle escalations.

4.2 Integration Interfaces
- Payment gateway for online interface
- National ID database / digilocker integration for ID verification.
- Police verification system for background checks.

5. Performance Requirements

5.1 Response Time
- Form submission & page loads within 3 seconds.
- Application status retrival within 2 seconds.

5.2 Scalability
- support for 500000 concurrent users and handle

Page No.

Date __/__/____

lakhs of applications annually.

5.3 Data Integrity
- No unauthorized modification of records.
- Automated backups and checksum validation for accuracy.

6. Design constraints
6.1 Hardware limitations
- Standard web servers with scalable cloud infrastructure.
- Biometric devices required at application centres.

6.2 Software Limitations
- Must run on secure web servers and must comply with government mandated encrypted standards.
- Must integrate with government approved database.

7. Non Functional Attributes
7.1 Security : Multifactor authentication for officials and encrypted data transmission & storage with Role based access control.

7.2 Reliability : Ensure high availability and fault tolerance to minimize system downtime.

7.3 Scalability : Cloud based architecture for future expansion.

7.4 Portability : Accessible on desktops & mobile devices with cross browser compatibility.

7.5 Usability : Simple, multilingual interface for applicants with accessibility compliance.

Saathi

Date ___ / ___ / _____

7.6 Reusability : Modular services like payment, verification, notification reusable in other e-governance projects

7.7 Compatibility : compatible with biometric scanners IP verification APIs and e-payment systems.

7.8 Data Integrity : Full audit logs of every transactions and immutable record storage for legal compliance.

8. Preliminary Schedule & Budget

The development of Passport Authentication System is estimated to take 6 months a budget of $530000 along with deployment phases.

P 22/8