Passport Authentication System

Introduction

Purpose of this Document:

To describe the requirements for a passport authentication system that verifies passport authenticity during immigration and border control.

Scope of this document

The system will automate passport verification and fraud detection, reducing manual intervention. Development cost and time will also be provided.

Overview:

The passport authentication system will cross-check passports with a central database, verify user credentials and flag any inconsistencies.

General Description:

The system will be used by immigration officers to authenticate passports at border checkpoints. It includes automated fraud detection features.

Functional Requirements:

- Passport data scanning and validation
- Cross-checking with international databases
- Fraud detection

Interface Requirements

- Integration with scanning devices
- Database connection for real-time passport verification
- Secure API for immigration data

Performance Requirements:

- Verification should be completed ~~within~~ within 2 sec
- Handle up to 50,000 daily verifications
- Maintain 99.9% accuracy in fraud detection

Design Constraint:

- ~~Must~~ Limited to approved passport scanning device
- Data privacy laws must be adhered to
- Must comply with international standards

Non-Functional Attributes

- High security and encryption for passport data.
- Reliable with 99.9% uptime
- Scalable for high-volume traffic during peak seasons.

Preliminary Schedule and Budget

- Development time: 6 months
- Estimated budget: ₹5,60,000