(5)   Passport Authentication:

1. Introduction-

1.1 Purpose: Outlines requirements for PAS. It serves to provide clarity on the system's objectives, functionalities and design considerations.

1.2 Scope: Overall workings and objectives of PAS, highlighting its value to users, including: enhanced security and streamlined processing.

1.3 Overview: to verify authenticity of passports and facilitate secure access to services requiring identity verification.

2. General Description-

↳ users need to authenticate passports, verify identity and access services securely.

↳ users typically basic understanding of biometric systems.

3. Functional Requirements

① passport scanning:
system shall allow users to scan passports using OCR

② Biometric Data Capture:
system shall capture and process biometric data.

③ Database Verification:
system shall verify the scanned passport against a
secure database

④ User Management:
system shall provide role-based access for government

⑤ Reporting:
system shall generate reports on authentication
activities and system usage.

4. Interface Requirements:
① User Interface - web-based interface for easy access.
② Data Interface - shall interface with national passport
databases

5. Performance Requirements:
① Scalability: Response-time: open applications within 2s
② Memory usage & error rate.

6. Design Constraints:
① Database - Utilize
② hardware limitations.

7. Non-Functional Requirements;
① Security: Data encryption
② Scalability: handled increase in data volume.
③ portability: accessible to all devices.

8. preliminary schedule & Budget:

- Total estimated Duration : 21 weeks

- Total estimated cost : & 11000

15/10/24