Nitte Meenakshi Institute of Technology

(AN AUTONOMOUS INSTITUTION AFFILIATED TO VISVESVARAYA TECHNOLOGICAL UNIVERSITY, BELGAUM)
PB No. 6429, Yelahanka, Bangalore 560-064, Karnataka
Telephone: 080- 22167800, 22167860
Fax: 080 – 22167805

Department of Information Science and Engineering

Software Engineering Lab Report <#>

Subject and Code: Software Engineering / 22ISG43 **Semester/ Section: 4 / C**
lAB Assigned Date: <28/05/2024> **Submitted Date: <28/05/2024>**
Faculty Name: Prof. A Balachandra / Ms Vaniv E S

Write the software requirements specifications for the problem statement IEEE 830 for a government agency to citizen registration and identification

1.Introduction
purpose:is to provide a detailed description of the software requirements for the development of a system to manage citizen registration and identification for a government agency.
Scope:the system aims to streamline the process of citizen registration and identification,enabling efficient data management The system aims to streamline the process of citizen registration and identification, enabling efficient data management and retrieval. It will facilitate the registration of new citizens, updating of existing citizen information, and verification of identity for various government services.

2. Overall Description
2.1 Product Perspective
The system will serve as a centralized platform for managing citizen information. It will integrate with existing government databases and systems to ensure data consistency and interoperability. The system will be accessible to authorized government personnel and may also provide limited access to citizens for self-service functionalities.

2.2 Product Features
• Citizen Registration: The system will allow government personnel to register new citizens by collecting relevant personal information and supporting documentation.
• Citizen Information Update: Authorized personnel can update citizen records to reflect changes in personal details or status.
• Identity Verification: The system will provide identity verification services to confirm the authenticity of citizen information for various government transactions.
• Reporting and Analytics: The system will generate reports and analytics on citizen demographics, registration trends, and other relevant metrics to support decision-making.

User Classes and Characteristics
• Administrators: Government personnel responsible for managing citizen registration and identification.
• Citizens: Individuals interacting with the system for registration or verification purposes.

Specific Requirements
3.1 Functional Requirements
3.1.1 User Authentication
• The system shall require users to authenticate themselves using unique credentials (example:username and password) to access functionalities.
• It shall support role-based access control to enforce appropriate privileges for different user roles.

3.1.2 Citizen Registration
• The system shall allow administrators to input and store personal information of new citizens, including but not limited to name, address, date of birth, and biometric data.
• It shall support the attachment and verification of supporting documents, such as birth certificates and identification proofs.

3.1.3 Citizen Information Update
• Authorized personnel shall be able to update citizen records to reflect changes in personal details, such as address or marital status.
• The system shall maintain a log of all changes made to citizen records, including timestamps and user identifiers.

3.1.4 Identity Verification
• The system shall provide identity verification services to authenticate citizen information against authoritative sources.
• It shall support integration with external databases and systems for identity verification purposes.

3.1.5 Reporting and Analytics
• The system shall generate customizable reports on citizen demographics, registration statistics, and other relevant metrics.
• It shall provide data visualization tools to present reports in a user-friendly format.

3.2 Non-Functional Requirements
3.2.1 Security
• The system shall adhere to industry-standard security practices to safeguard citizen data against unauthorized access, modification, or disclosure.
• It shall support encryption of sensitive data both in transit and at rest.

3.2.2 Performance
• The system shall be capable of handling a large volume of concurrent user requests without significant degradation in performance.
• It shall have a response time of no more than five seconds for standard user operations.

3.2.3 Reliability
• The system shall maintain high availability, with a target uptime of at least 99.9%.
• It shall implement mechanisms for data backup and disaster recovery to ensure data integrity and continuity of service.

3.2.4 Usability
• The system shall have an intuitive user interface with clear navigation and user-friendly input forms.
• It shall provide contextual help and guidance to assist users in completing tasks efficiently.

4. Other Requirements
4.1 Legal and Regulatory Compliance
• The system shall comply with all relevant laws and regulations pertaining to citizen data privacy and security.
• It shall support data retention policies mandated by regulatory authorities.

4.2 Documentation
• The system shall be accompanied by comprehensive user manuals and technical documentation to facilitate system administration and usage.

• It shall include training materials for users to familiarize themselves with system functionalities.

5. Glossary

This section shall provide definitions for key terms and acronyms used throughout the document.

6. Appendix

This section may include supplementary information such as mockups, diagrams, and additional requirements not covered in the main body of the document.