Software Requirements Specification (SRS)

Project Title: SmartGov Access System

Version: 1.0
Author: Nader Elabed
Date: July 2025

---

1. Introduction

1.1 Purpose

The purpose of this document is to define the functional and non-functional specifications for the SmartGov Access System: a secure, biometric and NFC-based platform for accessing digital government services and making authenticated payments.

1.2 Scope

This system allows users to:

- Authenticate using biometric identifiers (fingerprint or iris scan)
- Request government services (e.g., birth certificate issuance)
- Authorize and execute payments via NFC (smart card or linked bank account)
- Support delegated access with biometric approval from payer

1.3 Audience

- Developers
- System Architects
- Product Owners
- Government Digital Service Teams

---

2. Overall Description

2.1 Product Perspective

The system will be modular and API-centric, composed of:

- Biometric authentication module

- Government service request module
- NFC-based payment engine
- Admin dashboard (optional)

2.2 Product Functions

- Authenticate user identity biometrically
- Present available services
- Confirm payment via NFC card (linked to a verified identity)
- Support multi-party approval (requester and payer)

2.3 User Classes

- **Citizen**: Requests services, authenticates, initiates payments
- **Payer (optional)**: Approves payments with biometric validation
- **Admin**: Reviews logs and monitors transactions

2.4 Operating Environment

- Web application (desktop/mobile)
- NFC-compatible hardware or simulation tools
- Internet-connected environment

2.5 Assumptions & Dependencies

- NFC simulations will be used for PoC
- Biometrics will be mocked initially (HTML button or camera input)
- Payment gateway will be simulated

---

3. System Features

3.1 Biometric Authentication

- Users must provide a fingerprint or iris scan to access any service.
- A mock API will simulate biometric check.
- Tokens will be issued for successful authentication.

3.2 Government Services

- Users choose from a list of services (e.g., birth certificate, ID renewal).
- Each service includes: service ID, name, fee, documentation needed.
- Service request is validated and stored with metadata.

3.3 NFC Payment Authorization

- Payment only possible after authentication
- User taps NFC-enabled card or mobile wallet
- The system verifies card ownership via biometric token
- Payment record is saved and linked to the request

3.4 Delegated Payment

- A different person may pay on behalf of the requester
- Payer must authenticate biometrically
- Consent is logged and time-stamped

3.5 Logging and Audit

- All authentication and payment attempts are logged
- Failed biometric attempts are monitored
- Service records can be exported

---

4. Non-Functional Requirements

ID	Requirement
NFR-1	Response time for service request < 2s
NFR-2	Authentication and payment fully encrypted
NFR-3	Biometric data not stored in raw format
NFR-4	99.5% availability for core services
NFR-5	All logs retained for 90 days minimum

5. External Interfaces

5.1 User Interface

- Frontend: React or HTML/CSS
- Service selection UI
- Biometric check button or input
- NFC tap confirmation view
- Payment status screen

5.2 API Interface

- **POST /authenticate** – Validates biometric input
- **GET /services** – Lists all available services
- **POST /request-service** – Initiates service request
- **POST /pay** – Confirms NFC payment
- **POST /approve-payment** – Biometric approval for third-party

5.3 Database Interface

- PostgreSQL / MongoDB for persistence
- Tables: Users, Requests, Payments, Logs

5.4 Hardware Interface

- NFC reader or NFC mobile emulator
- (Optional) Biometric scanner or camera input simulation

---

6. Data Requirements

Table	Fields
Users	user_id, name, national_id, biometric_hash
Services	service_id, name, fee, status

Table	Fields
Requests	request_id, user_id, service_id, timestamp, status
Payments	payment_id, request_id, payer_id, method, timestamp, status
Logs	log_id, type, user_id, event, timestamp

7. Constraints

- Must comply with data privacy and security standards
- Biometric data must never be stored as plain text
- Use simulation tools only in development mode

8. Future Enhancements

- Integration with real biometric hardware
- Support for facial recognition
- Direct API link to e-Government systems
- Blockchain audit trail for transactions

9. Approval & Version History

Version	Date	Changes
1.0	July 2025	Initial version created by Nader Elabed

End of SRS Document