System Requirements Specification (SRS)

Project: Designing a National Integrated SGBV & TFGBV Case Management Platform

Candidate Name: Mohamed Fihaas

Role: Business Analyst

Table of Contents

1. Introduction

1.1 Project Title

National Integrated Case Management Platform for Sexual and Gender-Based Violence (SGBV) and Technology-Facilitated Gender-Based Violence (TFGBV)

1.2 Purpose

This project aims to create a centralized digital platform that enables victims, citizens, and officers to report and manage SGBV and TFGBV incidents through a single secure system.

The system will:

- Reduce victim frustration
- Prevent repeated storytelling of traumatic incidents
- Enable automatic case routing
- Improve inter-agency collaboration
- Securely manage evidence
- Increase response efficiency
- Protect victim privacy and confidentiality

2. Problem Understanding

Current Situation

Victims of SGBV and TFGBV in Sri Lanka currently face major challenges when attempting to report incidents.

Different organizations handle different categories of cases:

- Police Women & Children Bureau
- Cyber Crimes Investigation Division (CCID)
- National Child Protection Authority (NCPA)
- Ministry of Women & Child Affairs (MoWCA)
- Sri Lanka CERT (SLCERT)

Because responsibilities are distributed, victims are often redirected between institutions.

This creates:

- Emotional distress
- Delays in investigations
- Repeated storytelling of traumatic incidents
- Evidence loss
- Confusion about reporting channels
- Poor coordination between agencies

3. Objectives

Primary Objectives

1. Create a single national reporting platform.
2. Automatically route cases to the correct organizations.
3. Reduce re-victimization.
4. Enable secure multi-agency collaboration.
5. Securely store evidence.
6. Allow anonymous reporting.
7. Improve case tracking and transparency.

Business Objectives

- Improve operational efficiency
- Improve response times
- Improve accountability
- Improve citizen trust
- Standardize case handling workflows

4. Assumptions

1. All organizations agree to collaborate using a centralized system.
2. Government approval exists for secure inter-agency data sharing.
3. Citizens have access to internet-enabled devices.
4. The platform supports Sinhala, Tamil, and English.
5. Anonymous reporting is legally allowed.
6. Cases may involve multiple organizations simultaneously.
7. Evidence may include:
    - Images
    - Videos
    - Audio recordings
    - Chat screenshots
    - PDFs
8. Organizations will assign trained officers.
9. Each organization will maintain its own internal workflow hierarchy.
10. Cloud hosting infrastructure is available.
11. SMS and email services are available.
12. Role-based access control is mandatory.
13. Every system action must be logged.
14. Mobile responsiveness is required.
15. Sensitive victim information must remain encrypted.

5. Stakeholder Analysis

Stakeholder	Role
Victims / Citizens	Submit incidents and track cases
Police Women & Children Bureau	Handle physical abuse and protection cases
CCID	Handle cybercrime and online harassment
NCPA	Handle child abuse cases
MoWCA	Victim support and coordination
Sri Lanka CERT	Handle cybersecurity threats
Investigation Officers	Process and investigate cases
Supervisors	Review and approve escalations
System Administrators	Manage users and platform settings

6. Scope Definition

In Scope

- Incident reporting portal
- Anonymous reporting
- Evidence uploads
- Case management dashboard
- Case routing engine
- Multi-agency collaboration
- Notifications
- Audit logs
- Analytics dashboard

Out of Scope

- Court management systems
- Direct legal consultation
- Payment processing
- Social media monitoring automation

7. Functional Requirements

7.1 Public Reporting Portal

User Registration & Authentication

Features:

- Citizen registration
- OTP verification
- Secure login
- Anonymous reporting option

Incident Reporting

Users can:

- Select incident type
- Describe incidents
- Upload evidence
- Add location details
- Add suspect details
- Submit anonymously

Case Tracking

Users can:

- Track case status
- Receive notifications

- Upload additional evidence
- Communicate securely with officers

Emergency Support

Features:

- Emergency hotline integration
- Quick emergency reporting
- Safety resource information

7.2 Internal Case Management Portal

Officer Dashboard

Features:

- Assigned cases
- Pending approvals
- Escalated cases
- Notifications
- Performance summaries

Case Processing

Officers can:

- Review reports
- Update statuses
- Add notes
- Request additional evidence
- Escalate cases
- Reassign cases

Multi-Agency Collaboration

Features:

- Shared case access
- Secure messaging
- Joint investigations
- Cross-agency approvals

Evidence Management

Features:

- Encrypted evidence storage
- File previews
- Download restrictions
- Evidence audit tracking

Analytics Dashboard

Features:

- Case trends
- Region-wise statistics
- Organization workload
- Resolution performance

8. Non-Functional Requirements

Requirement Type	Description
Security	End-to-end encryption
Performance	Response time below 3 seconds
Availability	99.9% uptime
Scalability	National-level scalability
Accessibility	Mobile responsive UI
Localization	Sinhala, Tamil, English
Reliability	Automatic backup and recovery
Auditability	Complete audit logs
Compliance	Sri Lankan data privacy compliance
Usability	Simple user experience

9. User Roles & Permissions

Role	Permissions
Victim/User	Submit and track reports
Investigation Officer	Manage assigned cases
Supervisor	Approve escalations and closures
Organization Admin	Manage organization users
System Admin	Full platform administration

10. User Stories

Victim User Stories

- As a victim, I want to report incidents anonymously so that I can stay safe.
- As a victim, I want to upload screenshots and evidence so that investigators can understand my case.
- As a victim, I want to track my case status so that I know investigation progress.

Officer User Stories

- As an officer, I want automatic case routing so that cases reach the correct organization quickly.
- As an officer, I want secure evidence access so that sensitive information remains protected.
- As a supervisor, I want escalation controls so that urgent cases receive immediate attention.

11. Use Cases

Use Case 1: Anonymous Cyber Harassment Report

Actor

Victim

Flow

1. User opens reporting portal.
2. Selects anonymous reporting.
3. Uploads screenshots.
4. System categorizes case.
5. Case routed to CCID and SLCERT.
6. Officers begin investigation.

Use Case 2: Child Abuse Case

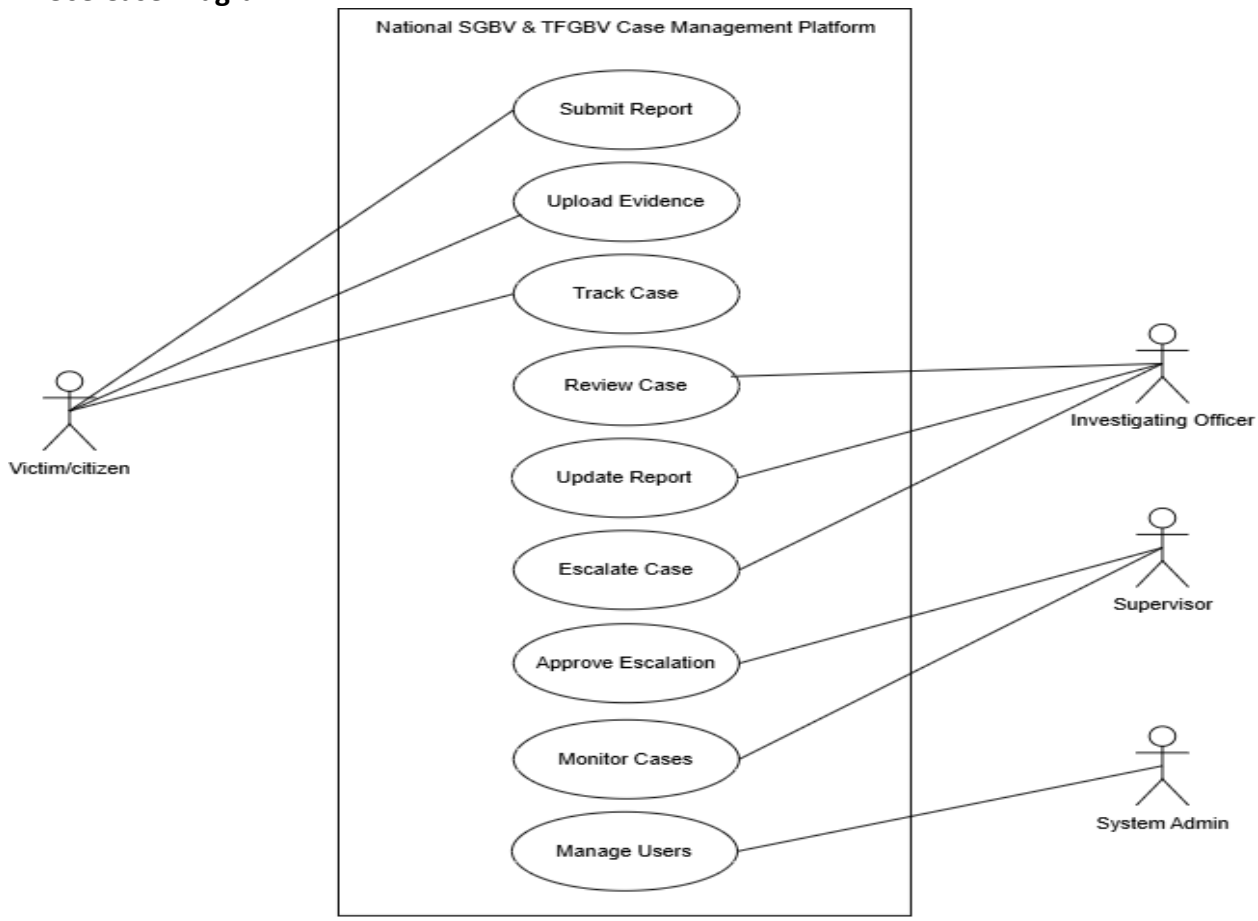
Actor

Citizen

Flow

1. Citizen reports child abuse.
2. System detects child-related category.
3. Case routed to:
    - NCPA
    - Police Women & Children Bureau
4. Joint investigation initiated.
5. Victim support services activated.

12. Use Case Diagram



13. Workflow Design

Step 1 — Incident Submission

Victim submits incident through public portal.

Step 2 — Automatic Classification

The system categorizes:

- Incident type
- Severity level
- Relevant organizations

Step 3 — Case Routing

The routing engine forwards the case to:

- Police
- CCID
- NCPA
- SLCERT
- MoWCA
  or multiple organizations.

Step 4 — Officer Review

Assigned officers review evidence and begin investigation.

Step 5 — Inter-Agency Collaboration

Organizations collaborate securely when required.

Step 6 — Case Resolution

Case status changes:

- Open
- Under Investigation
- Pending Evidence
- Escalated

- Resolved
- Closed

Step 7 — Victim Notification

Victim receives updates through:

- SMS
- Email
- In-app notifications

14. System Architecture

Major Components

Public Reporting Portal

Handles:

- Reporting
- Tracking
- Evidence uploads

API Gateway

Handles:

- Authentication
- Authorization
- Secure communication

Central Case Engine

Handles:

- Workflow management
- Case routing
- AI categorization

Organization Portals

Used by officers for:

- Case handling
- Collaboration
- Investigation management

Evidence Management Service

Handles:

- Secure evidence storage
- Encryption
- Audit trails

Notification Service

Handles:

- SMS
- Email
- Push notifications

15. Security & Privacy Requirements

Security Features

- End-to-end encryption
- Multi-factor authentication
- Role-based access control
- Secure APIs
- Evidence encryption
- Audit logs

Privacy Features

- Anonymous reporting
- Victim identity masking
- Restricted evidence access
- Secure communication channels

16. Risk Analysis

Risk	Mitigation
Data breach	Encryption
Unauthorized access	Role-based permissions
Evidence tampering	Immutable audit logs
Fake reporting	Verifications
System downtime	Cloud redundancy
Identity exposure	Data masking and restricted access

17. Wireframe Descriptions

Screen 1 — Public Home Page

Features:

- Emergency help button
- Start report button
- Track case option
- Language selector

Screen 2 — Incident Reporting Form

Fields:

- Incident category
- Description
- Date/time
- Location
- Evidence upload
- Anonymous reporting checkbox

Screen 3 — Case Tracking Page

Features:

- Enter case ID
- Track
- Timeline view

Screen 4 — Officer Dashboard

Widgets:

- Assigned cases
- Urgent cases
- Notifications

Screen 5 — Case Details Page

Sections:

- Victim details
- Evidence panel
- Activity timeline

- Investigation notes
- Incident Details

Screen 6 — Analytics Dashboard

Charts:

- Cases by region
- Cases by category
- Resolution timelines
- Agency workload

18. Suggested Technology Stack

Layer	**Technology**
Frontend	React / Next.js
Backend	Node.js / .NET
Database	PostgreSQL
File Storage	Secure cloud object storage
Authentication	OAuth2 + MFA
Hosting	Government cloud / AWS
Notifications	SMS gateway + email service

19. Agile BA Approach

Requirement Gathering

Methods:

- Stakeholder interviews
- Workshops
- Requirement analysis sessions

Agile Development Approach

Recommended methodology:

- Agile Scrum

Suggested sprint structure:

- Sprint duration: 2 weeks
- Sprint reviews
- Backlog prioritization
- Continuous feedback cycles

Prioritization Approach

High Priority Features

- Reporting portal
- Case routing
- Evidence management
- Role-based access

Medium Priority Features

- Analytics dashboards
- Secure messaging
- Multi-language support

Future Features

- AI categorization

- Chatbot assistance
- Mobile application

20. Future Enhancements

Potential future improvements:

- AI-powered risk detection
- Sentiment analysis
- GIS crime mapping
- Voice-based reporting
- Court system integration
- WhatsApp reporting integration
- Predictive analytics
- Blockchain evidence integrity

21. Conclusion

The proposed National Integrated SGBV & TFGBV Case Management Platform provides a centralized, secure, and victim-centered solution for handling sensitive incidents across multiple government organizations.

The solution improves:

- Accessibility
- Coordination
- Investigation efficiency
- Victim protection
- Transparency
- Accountability

By combining secure case management, automated routing, evidence handling, and multi-agency collaboration, the platform can significantly reduce victim frustration while improving the overall effectiveness of incident response in Sri Lanka.