Software Requirements Specification

Version 1.0

September 21, 2021

Vaccine Management System

Sankalp Kumar (skumar26@umd.edu)

Submitted in partial fulfillment
Of the requirements of
ENPM809W

<<Any comments inside double brackets such as these are *not* part of this SRS but are comments upon this SRS example to help the reader understand the point being made.

This work is based upon the submissions of the fall 2021 ENPM809W. The student who submitted the project is Sankalp Kumar>>

1.0. Introduction

1.1. Purpose

The purpose of this document is to present a detailed description of the Vaccine Management System. It will explain the purpose and features of the system, the interfaces of the system, what the system will do, the constraints under which it must operate and how the system will react to external stimuli. This document is intended to show case Secure Software Development Life Cycle while building the aforementioned software.

1.2. Scope of Project

The Project aims to build a Software that could be used by a government agency to track, manage, and run free vaccination drives on a large scale. The project will run as a web-based application allowing users to schedule their vaccine appointments.

2.0 Functional Requirements

2.1 Requirements

2.1.0 Signup

Description	Admins and Users both need to be Sign up before being able to login to the application.
Steps	1: Go to the URL of the application, different URLs depending on admin or user. 2: Click on signup. 3: Enter details. 4: Verify by clicking on the link in the email used to sign up.

2.1.1 Login

Description	The login can be done by both admins and users. Admin gets more privilege than the user. A different URL should be used to register,

	authenticate, and provide access to the admins.
Steps	1: Go to the URL of the application, different URLs depending on admin or user. 2: Click on Sign in. 3: Enter username and password. 4: If admin then enter 5: Click on login.

2.1.2 Adding vaccine centers

Description	The admin should be able to add vaccine centers followed by available vaccines, quantity, working hours of the center. Admin should be asked to enter all relevant information regarding the vaccine center.
Steps	1: In the admin page after logging in. 2: Add the vaccine center name. 3: Fill the form with all relevant information. 4: Click on add button.

2.1.3 Feedback

Description	A page needs to be implemented whereby user can send feedback to the agency managing the vaccination campaign. The user should be able to provide the feedback. For the 1.0 release no edit option will be provided. The admin should be able to see all the feedbacks.
Steps	1: User can click on navigate button to go the feedback page. 2: Enter their feedback. 3: Click on the submit button.

2.1.4 Booking appointments

Description	After the user has access to the website, they can enter a zip code and find the vaccine center and choose their desired

	time of the appointment. User can choose anytime; the expectation is that the strengthen on the vaccination center will be managed accordingly by the admins or the government agency running the campaign. The user also gets an option to choose which vaccine they want to get if a selection is available
Steps	1: Select booking from the navigation tabs. 2: Enter the zip code. 3: Select from available vaccine options and enter the time for appointment. 4: Click on book button.

2.1.5 Certificates

Description	The system should produce a certificate for the user upon getting vaccinated. The certificate can be downloaded by the user and must be in PDF format.
Steps	1: Select booking from the navigation tabs. 2: Click on the certificate button.

2.1.6 Send Reminder

Description	The application needs to send a reminder email to the user exactly at 7:00AM on the appointment day.
Steps	1: The system notes down the time of the booking. 2: Sends an automated email.

2.1.7 Verify a certificate

Description	The application provides a certificate upload option where the admin could upload to check if a certificate is valid or not.
Steps	1: Go to the verification tab 2: Upload certificate 3: Click on Submit

3.0. Overall Description

3.1 System Environment

Vaccine Management System will have two users the admin and the User. User is any ordinary person trying to book a vaccine appointment whereas Admins are the ones running a particular vaccination drive. The application runs as web-based service allowing for the below use cases. Certain tasks will also be performed automatically by the software system and the actor has been called System or Application interchangeably throughout the document.

The admins running the campaign are expected to be tech savvy to be able to run and deploy the binary provided on their own central server. Server Management and deploying external security measures are the responsibility of the admins. Although there are some required measures as well as advice that have been covered in this document.

3.2 Detailed Use cases and Misuse Cases

3.2.1 Admin Perspective Use cases

The admin should be able to securely login into the system and be able to:

A. To be able to register and login into the system
B. Add a new vaccination campaign.
C. Run simultaneous vaccine drives.
D. Upload vaccine options available, quantity, the Centers, and timings.
E. Receive feedback on their vaccination campaign.
F. Verify a certificate.

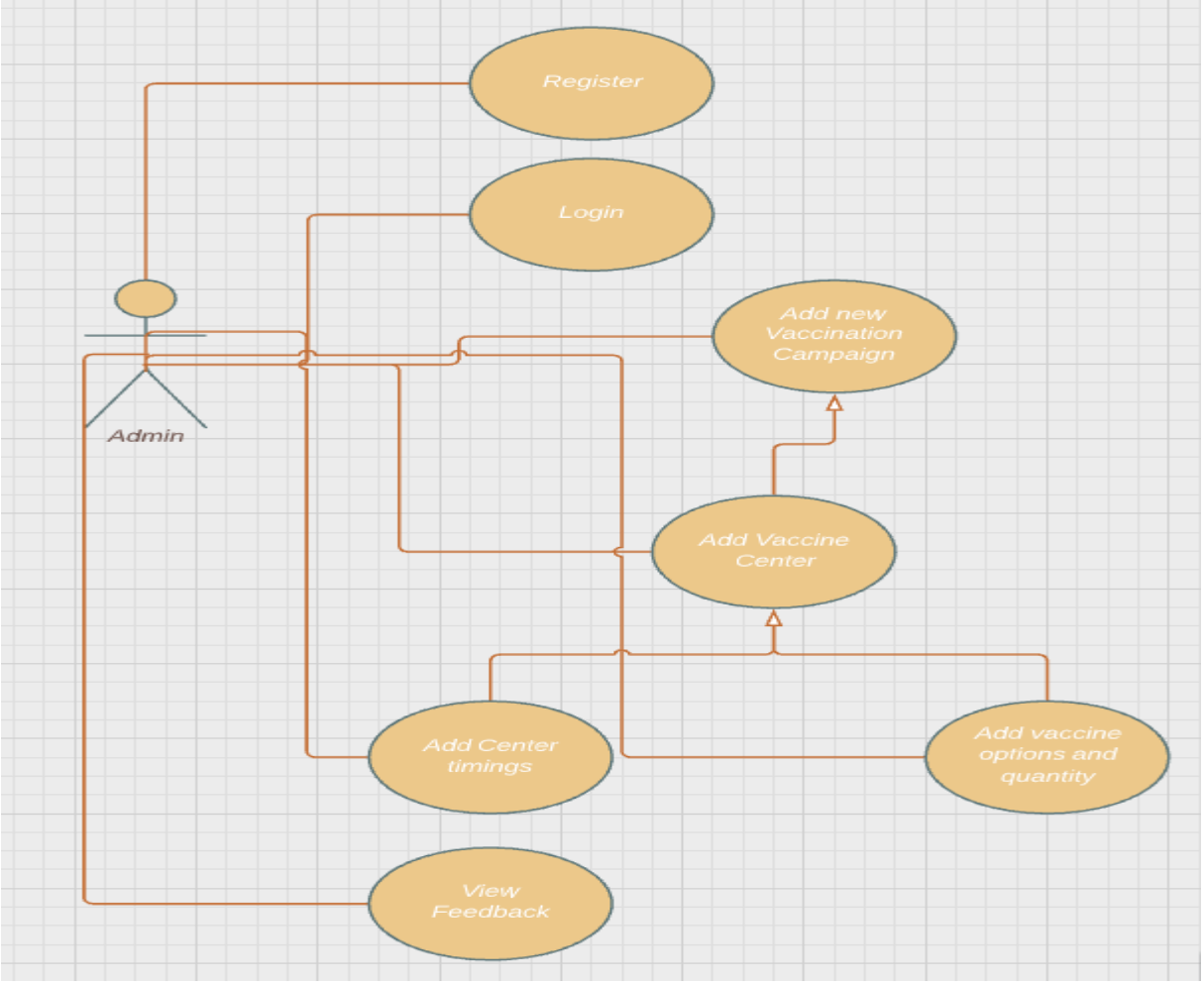

Figure 1 : Use case diagram for admin

3.2.2 Admin Misuse cases

Insider attacks are rampant, and admins can't be trusted. Since admins are the ones having more privilege than an ordinary user, there must be stringent security posture to ensure no misuse.

A: An admins identity must be verified. Spoofing of Admin Identity must be protected against.

B: Admins can't be trusted either, their mischievous actions must be scrutinized.

C: Admins are allowed to create vaccine campaigns; this could be misused to overwhelm the server by creating infinite campaigns.

D: Admins can attempt to change data which they are not allowed to edit such as certificates, feedback etc.

E: Admins can attempt to get access to data that is sensitive such as User's personal information, their account passwords etc.

F: Could also create DOS attacks by changing password of users.

G: Admin passwords could be compromised putting the entire vaccination campaign in jeopardy.

H: Admins could run reverse engineering on the software provided to learn more about the software.

3.2.3 User Perspective Use cases

The user should be able to login and perform the following:

A. Register their accounts.
B. Login to the application.
C. Should be able to book an appointment at a desired location by providing a zip code.
D. Choose their desired vaccine option
E. Should be able to provide feedback.
F. Should receive an email notification.

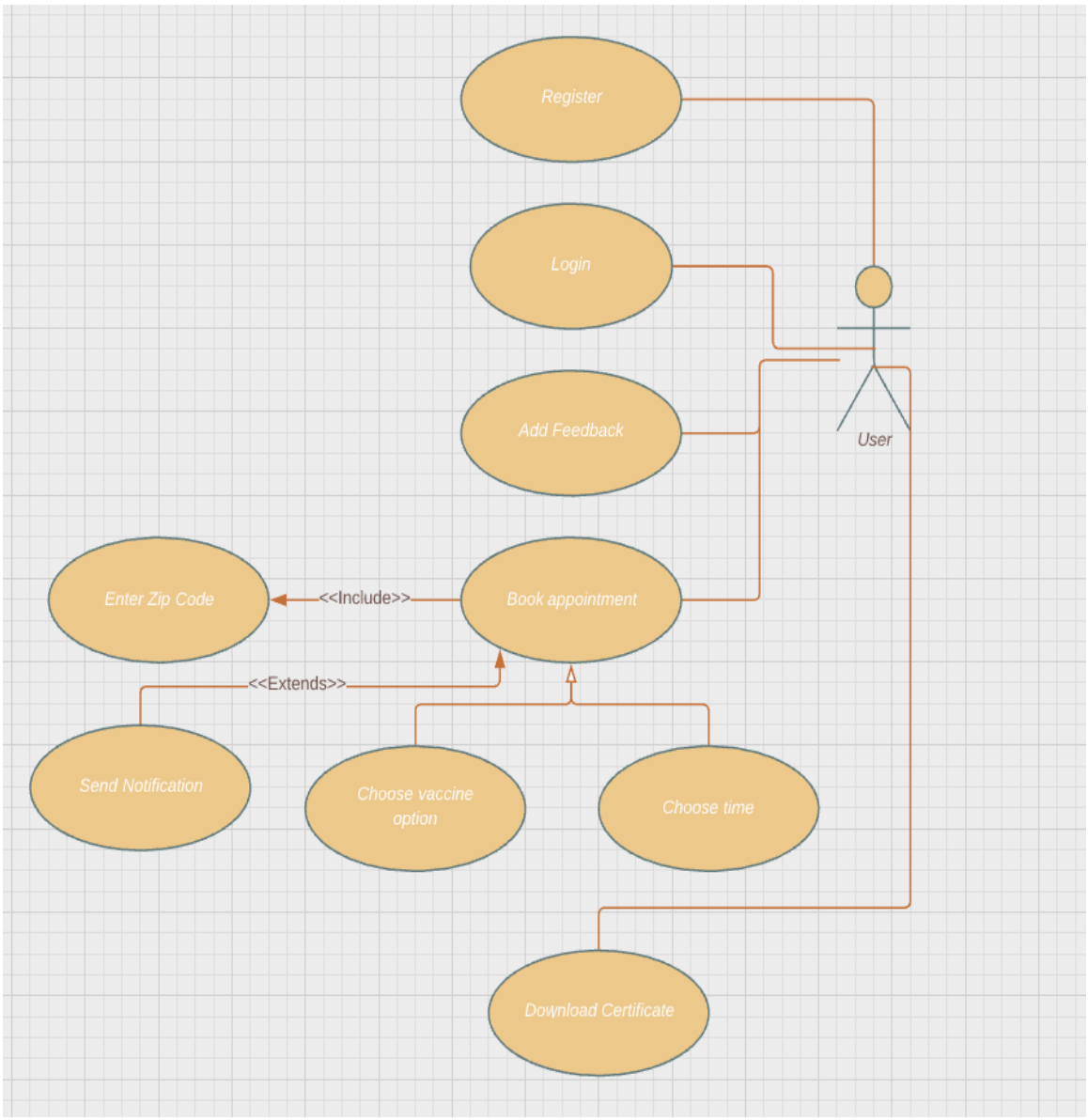

Figure 2: Use case diagram for user

3.2.4 User Misuse cases

A: User could spoof their identity just like admins.

B: User could perform mischievous activity using their account.

C: User could try and forge vaccine certificates.

D: User could overwhelm the system by booking infinite vaccine appointments.

E: User could book an appointment and not actually attend the appointment but could claim they have attended.

F: User could try and elevate their privilege to that of the admins.

G: The user could Add fake feedback without attending the appointment.

H: The user could try and look up all the zip code of a country to get information about all possible vaccination centers. Although not detrimental to the application but such information gathering could be part of a larger attack that could be carried out in person.

3.2.5 Application Use cases

The application software is responsible for the following use cases:

A: Generate Vaccine certificates.

B: Send reminder a day before to attend the appointment.

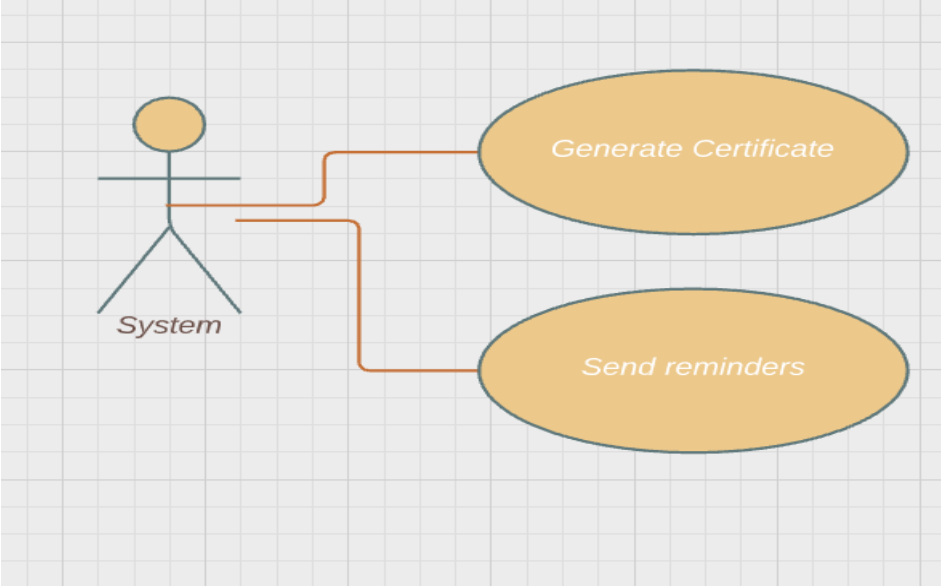

Figure 3: Application use cases

3.2.6 Application Misuse cases

A: Duplication of vaccine certificate; rogue admin and users can attempt to create fake certificates.

B: The reminder use case could be used by a rogue user to create dos attacks on other SMTP servers by registering the same email again.

C: An attacker could manipulate the time so that the system does not send the reminder on time.

3.2.7 Database Design

The database would store information for each admin, user and vaccination campaign. This is basic data that we need store and is expected to undergo changes in the design document after we make a consideration on security requirements. It is intended to give brief overview of the database and help user to appreciate the changes that will be showcased later in the design document.

3.2.7.1 Admin table

Name	Email	Password

Name: This is the name of the admin.
Email: This is the official email Id that will be used by admins to register.
Password: This is the password that will be used by Admin.

Email of the admin must be unique.

3.2.7.2 Vaccine Campaign table

Center name	Zip Code	Vaccine name	Stock left	timings

Center name: This is the name of the center that will run some campaign.
Zip Code: This is the zip code of the center.
Vaccine name: The name of the vaccine available.
Stock left: The number of vaccines left.
Timings: The working hours of the vaccine center.
Zip code along with Center name should be unique.

3.2.7.3 User table

Name	GID	Email	Password	Address	Center name	Vaccine name	time	Feed back	Attended

Name: Name of the User
GID: This is the Government ID provided by the user.
Email: Email id that has been used by the user to register
Password: The password for the account entered by the user.
Address: The resident address of the user.
Center name: Name of the center where an appointment has been booked.
Vaccine name: The vaccine selected by the user.
Time: The time of the appointment.
Feedback: The feedback that the user provides on the vaccination campaign.

The email id of the user must be unique.

4.0 Security Requirements

This section covers defense that needs to be deployed against the misuse cases. It also provides an overall security posture that needs to be deployed to protect against threats that are beyond the scope of the development lifecycle of this software.

Microsoft's STRIDE has been used to categorize each of the misuse cases.

4.1 Spoofing attacks:

2.4.1.1 *User's Identity must be verified before trusting.*
Spoofing could have multiple implications on the system:
A: This could lead to a rogue user performing actions on the system with no log information of the attacker present.
B: Could attempt to launch a DOS using our system by putting same email while registering when we send confirmation/reminder mails. B will be covered under Denial-of-Service Later

2.4.1.2 *Admins Identity must be verified before giving access to the system.*
Admins having more privilege than an ordinary user since they are the ones updating the vaccine centers. Hence, it is pertinent that we verify them before trusting.
Defense:
Both user and admins need to verify their email to be granted access to the application. If they do not verify using their email, they will not be granted access.

The admin needs to further use two factor authentication to be able to login. This is a good to have security feature for the first release. Admin pages are only to be accessible inside the agency managing the server. Hence, the agency is also responsible to ensure only legitimate people have access to their network.

4.2 Tampering of the data:

2.4.2.1 *The tampering of the database could be done by the admins:*
Defense:

Feedback and other information belonging to user must be entered only by users and admins should not have access to do so.

2.4.2.2 *certificate forging:*
Defense:
Certificates will be signed using a Private Key. These private keys must be created by the Application and kept securely.

2.4.2.3 *A user could add feedback without attending the meeting:*
Defense:
Feedback should only be allowed once it has been confirmed that the user did attend the appointment.

4.3 Repudiation:

2.4.3.1 Logging whether the appointment was obliged by the user:
Defense:
This is a severe problem to solve given that we want to keep things minimalistic to conserver development bandwidth. The system needs to generate a code 5 mins before the appointment which must be entered in a page that is accessible through admin. It is understood that we are trusting admins here and this has loopholes. In the future release this interaction will be limited and user's biometric will be stored and used.

2.4.3.2 *Non repudiating mischievous attempts by users and admins.*
Defense:
Track and log all the actions that are being executed by the Users and Admins. The information logged should be adequate to enough to decipher what actions were taken and who took these actions.

4.4 Information Disclosure:

4.4.1 *Admins can attempt to get access to sensitive data in the database such as User passwords.*
Defense:
All passwords must be hashed and salted before storing the databases.
All information must be stored in encrypted form in the database.
The access to the database will be protected by password that is known only to the Developer of the Vaccine management system.

4.4.2 *User could attempt to try look up all zip code to get information about all the vaccine centers.*
Defense:
A threshold must be decided upon and users violating this will be banned.

4.4.3 *Admins can try reverse engineering on the software binary provided to them.*
Defense:

Obfuscation techniques must be used to make reverse engineering difficult.

4.5 Denial of Service:

4.5.1 *Sending of email confirmations and reminders could be used to as a launch pad for DOS on others:*

Defense: No multiple booking appointment from the same user.

User should be allowed to book only one appointment for one vaccine.

4.5.2 *DOS attack by admins by attempting to create infinite vaccine campaigns.*

Defense: Number of vaccine campaigns to be run by the admin should be restricted.

4.5.3 *DOS attack by booking infinite vaccine appointments:*

Defense:

Limit the number of appointments for each User and ban them if an attempt is made to book more than the limit in a given time period. There is no functionality of cancelling the appointment.

4.5.3 *DDOS attack on the login page:*

Defense: for this cannot be provided through software mechanism, some advice has been put up to deal with this in section **2.4.12 External Security Deployment.**

4.5.4 *DOS attack by attempting to manipulate the time of the system to delay reminder emails:*

Defense: The time needs to be synchronized every 30 mins from a NIST Internet Time Servers. Plus incase a change in time is detected then all admins must be notified.

4.6 Escalation of Privilege:

2.4.6.1 *An ordinary user must not get admin Privileges*.

The easiest way to get access to an employee account is through brute force attack on the password if an attacker gets access to email of the admin through social engineering skills.

Defense:

The password needs to be long enough and should have special characters to make brute force attacks inefficient.

2.4.6.2 *Protection against compromised passwords:*

Defense:

Password management policies must be implemented whereby admins need to change password after a certain amount of time, a previously used password cannot be used.

A 2-factor authentication must be added for all the admins.

2.4.9: Privacy Compliance

Since we are storing user data, we must ensure we follow compliance that are applicable to the country.

2.4.10: Government Certifications:
As the software is intended to be used by Government agencies a government security certification will help the software to be guaranteed of being safe for usage. The aim is to meet the security criteria set.

2.4.12 Exposing only encrypted web interface:
Providing a secure interface to connect and avoid plain text message passing over the internet when a user accesses the website must be ensured through encryption protocols.

2.4.13 Protection of the Cryptographic Keys:
The crypto keys that will be used for encryption and certificate signing must be protected at all costs. The proposal is also to allow system to generate crypto keys every year and re-encrypt the database and re-sign the certificate again to ensure forward secrecy. The old certificates will no longer be valid, and the user needs to download their certificates again.

2.4.12 External Security Deployment:
Since the user of the system is responsible for managing their server and its security. Below is security advice for better posture. We do not get into any more details of the below suggested security products:
2.4.12.1 Secure Web Gateway deployment:
This is a network-based security device and provides network security at the gateway of your network.
2.4.12.2 Intrusion Prevent System or Next Generation Firewall Deployment:
Modern IPS supports TLS inspection and can find attacks in encrypted traffic using MITM proxy. They also give an option to deploy your own signature sets and will be useful for government agencies having their own security teams. The advice is to use Secure web gateway and IPS/NGFW from two different vendors to further strengthen the security posture.
2.4.12.3 WAF deployment:
Firewall for L7 traffic.
2.4.12.4 Cloudflare DDOS protection deployment:
Cloudflare provides its DDOS protection service which could be used to effectively mitigate attacks from large bot army.