Software Requirements Specification

for

Web Application for NIC

Version 1.0 approved

Ronald Tony (U101116FCS103)

Sourav Upadhya (U101116FCS134)

Saloni Jain (U101116FCS107)

Sourish Das (U101116FCS135)

Shubhangi (U101116FCS127)

Sabyasachi Mishra (U101116FCS104)

NIIT University

16th September 2018

Table of Contents

1. Introduction

1.1 Purpose

Web application for authorization of Wi-Fi services, which will be integrated with NIC's website. The web application will be a management system which will allow users to configure the devices using the organization's secure wireless services.

1.2 Document Conventions

-

1.3 Intended Audience and Reading Suggestions

- Course in charge
- Project manager
- Team members

1.4 Product Scope

Project aims to provide web application to manage the safe and secure wireless connection provided by the organization

BENEFITS

- Secure login.
- Easy management of devices accessing the wireless connection.

1.5 References

IEEE Recommended Practice for Software Requirements Specifications - Standard 830

2. Overall Description

2.1 Product Perspective

The current system for authenticating wireless connections to the users is done manually by submitting a written document; in order to ease this whole process, the web application is being developed.

2.2 Product Functions

- Adding new devices for accessing the organization's wireless services.
- Modify devices in case of any changes in the data provided for the registered devices.
- Remove devices in case the device won't use the organization's wireless services.

2.3 User Classes and Characteristics

- Employees
    - Works at the organization
- Administrators
    - Manages the services being used
    - Authorizes the user claiming for the services
- Guest Users
    - Doesn't work in the organization

2.4 Operating Environment

Web Browsers, no mobile compatibility. Runs a MySQL Database in back-end.

2.5 Design and Implementation Constraints

Project needs to be done using the following technologies:

- HTML
- CSS
- PHP
- JavaScript
- MySQL

2.6 User Documentation

Tutorials and manuals will be provided. They will be in the form of softcopy as well as hardcopy.

2.7 Assumptions and Dependencies

Project manager may ask to implement user authentication using Aadhaar or OTP system.

3. External Interface Requirements

3.1 User Interfaces

- Login Page
    - Username
    - Password
- Registration (For username and password)
- Home Page
    - Adding, modifying and removing devices

3.2 Hardware Interfaces

No specific hardware interfaces used.

3.3 Software Interfaces

Web Application will be utilizing phpMyAdmin to provide responses and connect the application to the database.

3.4 Communications Interfaces

- HTTP
- TCP/IP: For database connectivity of MySQL
- Unix socket file connection

4. System Features

4.1 Authentication (Client)

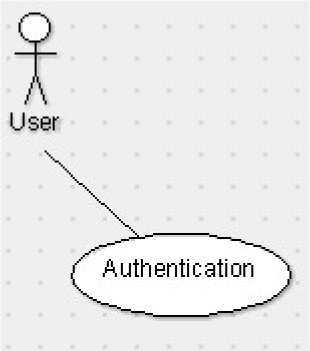
4.1.1 Description and Priority

- User authentication through username and password to enter user's dashboard
- High priority

4.1.2 Stimulus/Response Sequences

- User enters username and password.
- System will authenticate particular details with database and responses with OK code.
- In case of error, alerts with incorrect username and password.
- Redirects to user's dashboard in case of correct authentication.

4.1.3 Functional Requirements



User enters his user name and password which on authentication will redirect the user to his dashboard. The authentication sends the username as text and password as SHA1 encrypted code to the server. The server compares the details with the user database. In case of authentication failure, the user is given alert message stating incorrect username or password. The user is given 3 attempts to successfully authenticate himself.

4.2 Registration (Client)

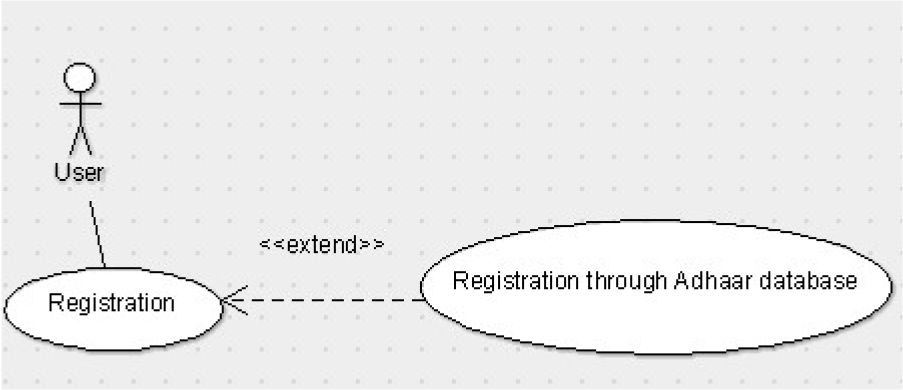
4.2.1 Description and Priority

- User registration through username, password and relevant user details
- Medium priority

4.2.2 Stimulus/Response Sequences

- User enters details, password is to be repeated
- System will validate the entered details
- In case of error, alerts with message
- Stores into the database
- Redirects login page in case of successful registration

4.2.3 Functional Requirements



The user, for his/her registration to the system, must provide name, address, contact details and Aadhaar number. The system validates the entered details and then stores into the system. In case of any error, the user is notified. On successful registration the user is redirected to the login page.

4.3 Adding Devices (Client - Dashboard)

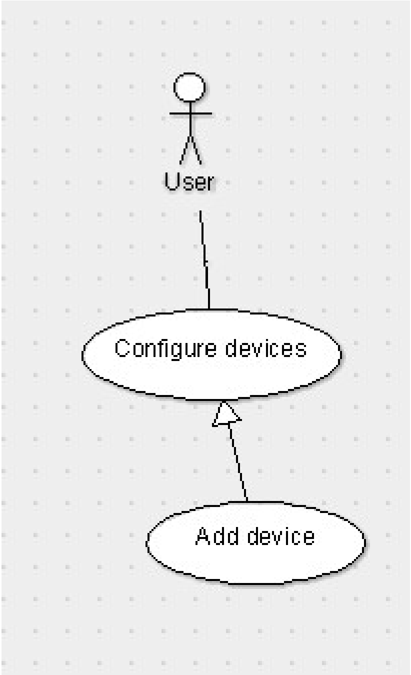
4.3.1 Description and Priority

- User registers his new device for using organization's secure wireless service
- Requires MAC-Address
- Medium priority

4.3.2 Stimulus/Response Sequences

- User enters new MAC-Address for the device
- System will validate the entered details
- In case of error, alerts with message
- Stores into the database and sends for administrative authentication of device and user details
- Redirects to user's dashboard in case of successful registration

4.3.3 Functional Requirements



User enters the MAC addresses of the new devices (up to three a time) that require to be connected. The device details are then sent to the administrative personnel who then authorize the device to use the organization's secure wireless services.

4.4 Modifying Devices (Client - Dashboard)

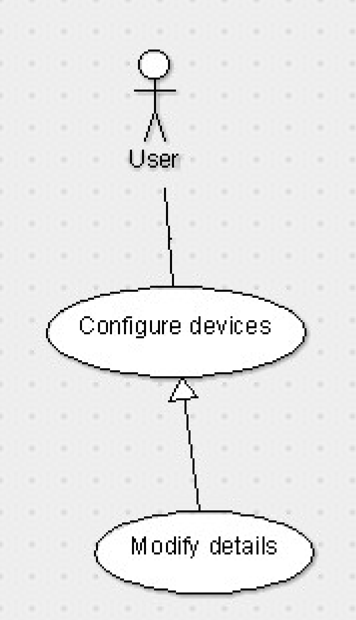
4.4.1 Description and Priority

- User modifies his existing device details
- Requires MAC-Address for new device(s)
- Medium priority

4.4.2 Stimulus/Response Sequences

- User enters new MAC-Address for the device.
- System will validate the entered details.
- In case of error, alerts with message.
- Stores into the database and sends for administrative authentication of device and user details.
- Redirects to user's dashboard in case of successful registration.

4.4.3 Functional Requirements



User enters the new MAC address of the device(s) that needs to be updated from the list of devices that are currently authorized to use the secure wireless connection. The new details are updated in the database and also sent for approval to the administrative personnel.

4.5 Removing Devices (Client - Dashboard)

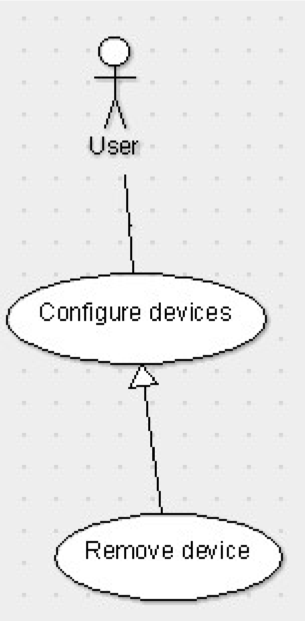
4.5.1 Description and Priority

- User removes device(s) under his account
- Requires to enter password
- Medium priority

4.5.2 Stimulus/Response Sequences

- User selects MAC-Addresses of the device(s)
- On selecting remove, administration will be informed of the same and address will be removed
- Redirects to user's dashboard in case of successful operation

4.5.3 Functional Requirements



In case the user wants to disconnect a device from the service, he/she must select the device(s) and enter his/her password when prompted to do so. The database is then updated with the new list of connected devices.

4.6 Search Registrations (Admin)

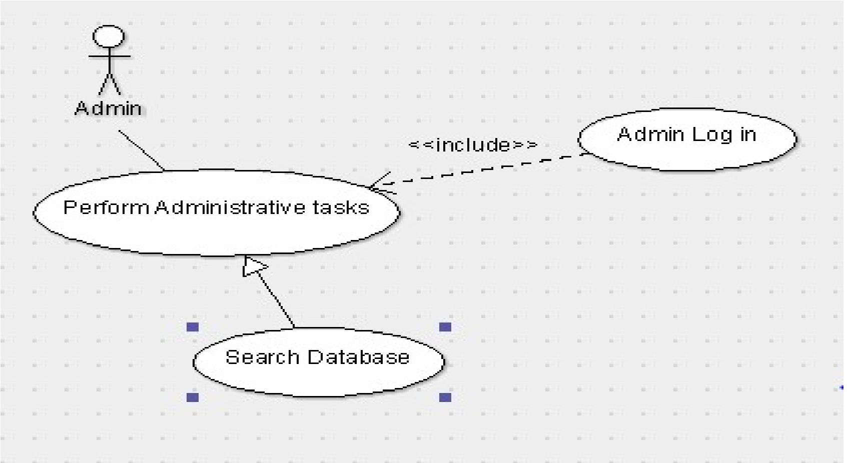
4.6.1 Description and Priority

- Admin can search for particular record(s) in registrations.
- Medium priority

4.6.2 Stimulus/Response Sequences

- Admin selects type of search and enters keywords.
- On selecting search, data requested will be displayed in tabular form if exists.

4.6.3 Functional Requirements



Administrator can search for particular records in database by selecting the type of search, for e.g., search by username, search by name, search by department, etc. and enter keywords of search. A table shows the required results, if the data exists.

4.7 Approve Devices (Admin)

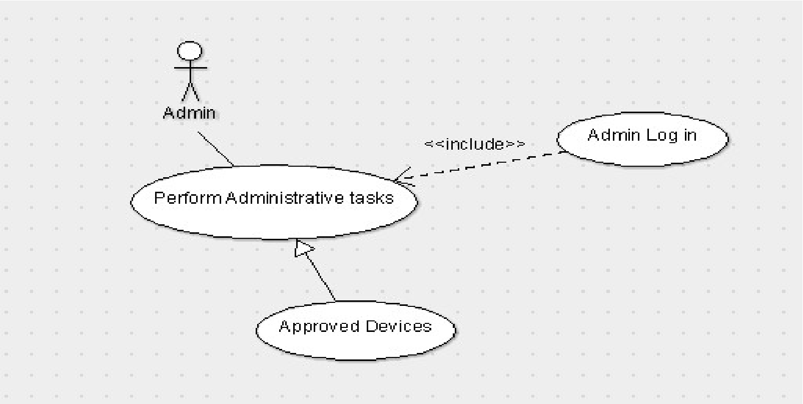
4.7.1 Description and Priority

- Admin can approve or decline requests for wireless connection of device(s).
- High priority

4.7.2 Stimulus/Response Sequences

- Admin views requests and verifies data.
- In case of valid data, admin selects device(s) and sets password for connection.
- This returns password for wireless connection to user.

4.7.3 Functional Requirements



Administrator views the request of device(s) for wireless connection. The data given is then validated and a password is then set for the given device(s). The User can then use the password to connect to the wireless service of the organization.

4.8 Remove Devices (Admin)

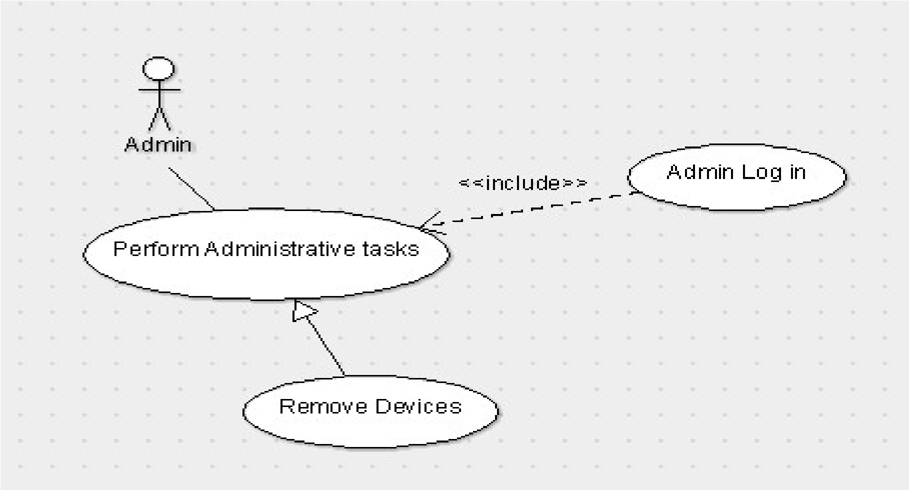
4.8.1 Description and Priority

- Admin can remove device(s) in case of violation of organization policies.
- Medium priority

4.8.2 Stimulus/Response Sequences

- Admin views approved device(s) and selects device to be removed.
- Selected device(s) are then removed from database.

4.8.3 Functional Requirements



In case of violations of policy by certain device(s) connected to the wireless service, the administrator selects device(s), and removes them from database. The device is then marked as removed by admin in user panel to indicate that the device is no longer supported to use the wireless service.

5. Other Nonfunctional Requirements

5.1 Performance Requirements

The system is expected to handle up to 100 user requests at a time.

5.2 Safety Requirements

No particular safety requirements.

5.3 Security Requirements

User authentication must be secure to access user's dashboard.

5.4 Software Quality Attributes

No particular software quality attributes.

5.5 Business Rules

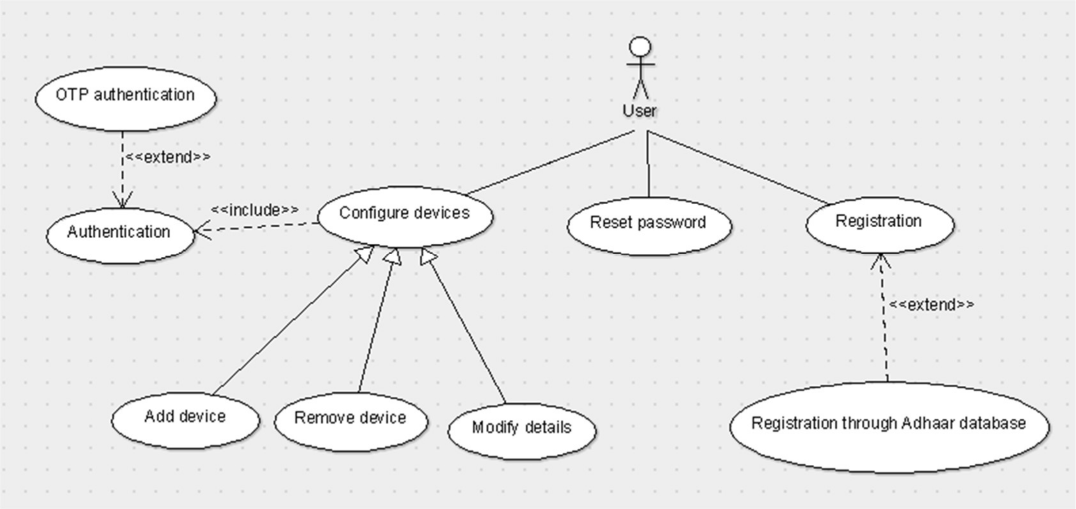
Web application must pass the organization's security audit.

Appendix A: Glossary

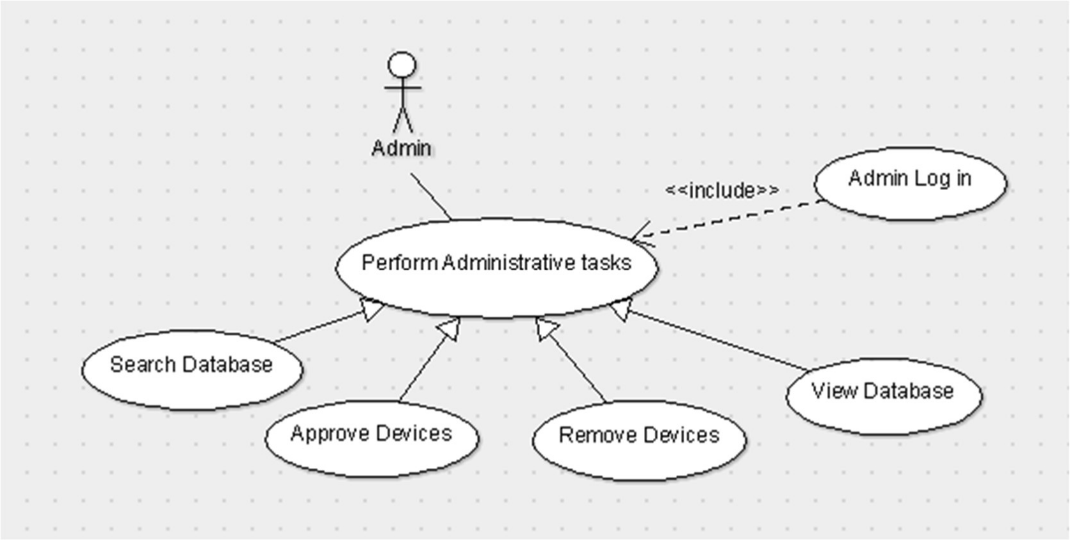
- SHA1 encryption:

  A cryptographic hash (sometimes called 'digest') is a kind of 'signature' for a text or a data file. SHA1 generates an almost-unique 160-bit (20-byte) signature for a text.

Appendix B: Analysis Model



Client - Side



Admin - Side