UC24 – System Admin Services - Security Management Use Case Specification

State of MN - eHEAT Phase III

Version 1.2

Revision History

Date	Version	Description	Author
02/22/2004	DRAFT	Initial Version	Subramani Muthu
02/22/2004	Version 1.0	Review complete with Narayan Srinivasan. Submitted for signoff	Subramani Muthu
05/06/2004	Version 1.1	Updated by Narayan Srinivasan: 1. Alternate Flow 4.1.3. Changed "Add User" action to "Create User" 2. Corrected typos	Narayan Srinivasan
08/04/2004	Version 1.2	1. Business rules section modified to include up to date security changes. 2. 4.1.5 – Section modified to include enable functionality. 3. 4.1.6 – Reset password functionality section added.	Sam Chidambaram

Table of Contents

System Admin Services - Security Management

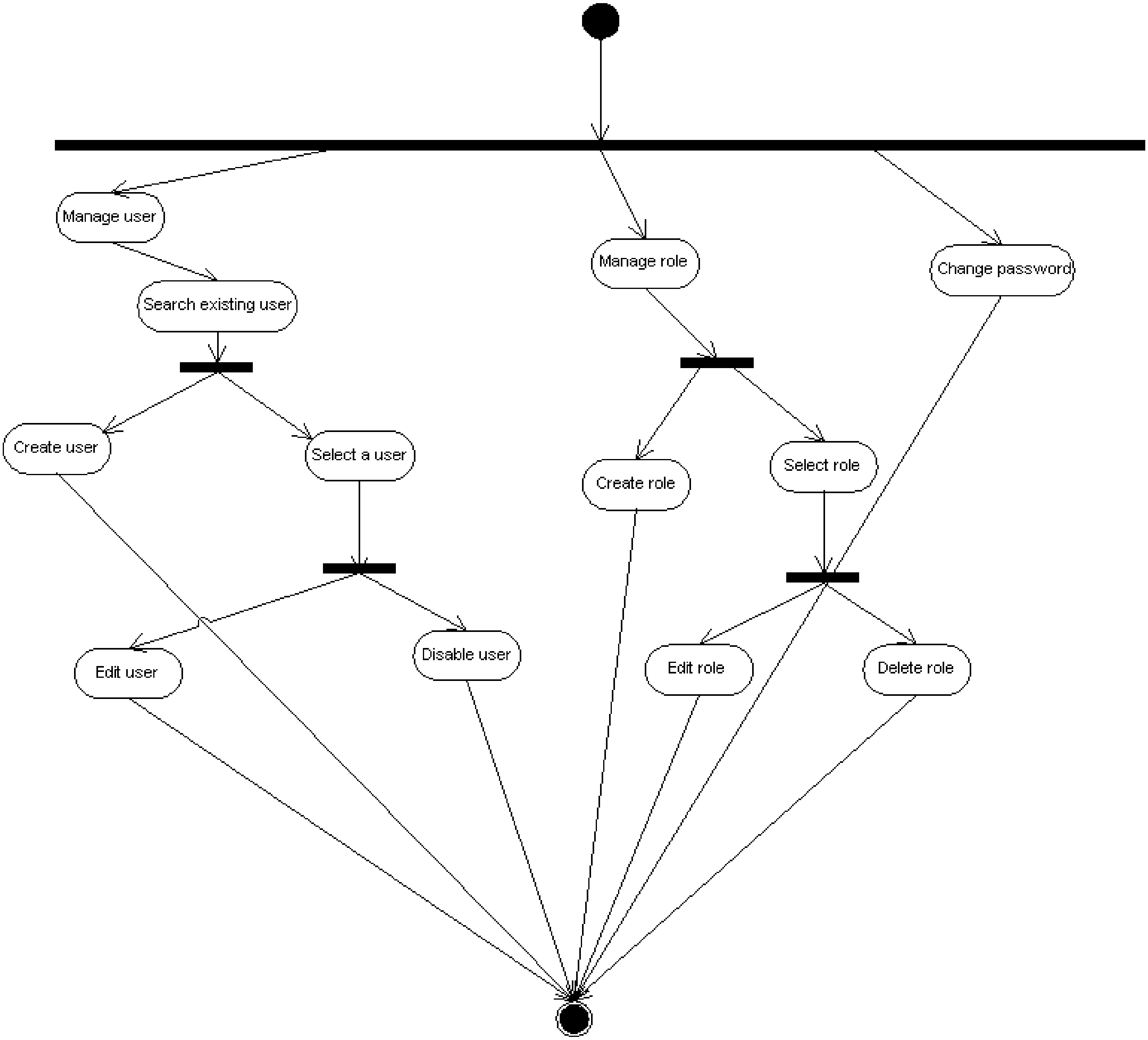
1. Brief Description

This use case provides a way to administer security in the eHEAT System.

2. Actors

Authorized DOC user

3. Activity Diagram



4 Flow of Events

4.1 Basic Flow – Manage User

4.1.1 Start of the Use Case

This use case starts when Authorized DOC user clicks “Manage User” from the “Security Management” tab from the “System Admin Services” menu.

4.1.2 Search user

1. System displays user search screen. Authorized DOC user enters one or more search criteria and clicks on the “Search” Button to initiate a search.
2. If records are found, the system displays the Search results in a list.
3. If no records are found –
    a. The system displays a message “No user found. Please select different search criteria”.
    b. The system will allow a new user to be created.

4.1.3 Create user

1. This alternate flow starts after the basic flow 4.1.2
2. On clicking the “Create User” button, system displays user information entry screen. Authorized DOC User enters all the information and clicks “Submit” button
3. On success, the system saves the user information and displays appropriate success message. If unsuccessful, the system displays appropriate error message.
4. When the user clicks the “Quit” button, the system will display the previous screen

4.1.4 Edit user

1. This alternate flow starts after the basic flow 4.1.2
2. On clicking “Edit User” button by selecting an existing user from the user id list, system displays user information edit screen for the selected user. Authorized DOC user enters all the information and clicks “Submit” button.
3. On success, the system saves the user information and displays appropriate success message. If unsuccessful, the system displays appropriate error message.
4. When the user clicks “Quit” button, the system will take the user to previous screen

4.1.5 Disable/Enable user

1. This alternate flow starts after the basic flow 4.1.2
2. On clicking “Disable/Enable User” button by selecting an existing user from the user id dropdown list, the system disables the selected user.
3. On success the system displays appropriate success message. If unsuccessful, the system displays appropriate error message.

4.1.6 Reset Password

1. This alternate flow starts after the basic flow 4.1.2
2. On clicking “Reset Password” button by selecting an existing user from the user id list, system displays reset password screen for the selected user. Authorized DOC user enters new password and clicks “Submit” button.
3. On clicking of “Submit” button the password will be reset to the new password entered.
4. On success the system displays appropriate success message. If unsuccessful, the system displays appropriate error message.

4.1.7 Use Case Ends

The use case ends on display of the message.

4.2 Alternate Flow – Manage Role

4.2.1 Manage Role

1. This alternate flow starts when Authorized DOC user clicks “Manage Role” from Security Management tab from System Admin services menu.

4.2.1.1 Create Role

1. On clicking “Add Role” button, system displays role information entry screen. Authorized DOC user enters all the information and clicks “Submit” button
2. On success the system saves the role information and displays appropriate success message. If unsuccessful, the system displays appropriate error message.
3. When the user clicks “Quit” button, the system will take the user to previous screen

4.2.1.2 Edit Role

1. On clicking “Edit Role” button by selecting an existing role from the role dropdown list, system displays role information edit screen for the selected role. Authorized DOC user enters all the information and clicks “Submit” button.
2. On success, the system saves the role information and displays appropriate success message. If unsuccessful, the system displays appropriate error message.
3. When the user clicks “Quit” button, the system will take the user to previous screen

4.2.1.3 Delete Role

1. On clicking “Delete Role” button by selecting an existing role from the role dropdown list, the system deletes the selected role.
2. On success the displays appropriate success message. If unsuccessful, the system displays appropriate error message.

4.3 Alternate Flow – Change Password

4.3.1 Change Password

1. This alternate flow starts when User clicks “Change Password” from Security Management tab from System Admin Services menu.
2. On clicking “Change Password”, system displays password information entry screen. User enters all the information and clicks “Submit” button
3. On success the system saves the new password and displays appropriate success message. If unsuccessful, the system displays appropriate error message.
4. When the user clicks “Quit” button, the system will take the user to previous screen

5 Special Requirements

None

6 Preconditions

Logged in user should be an Authorized DOC user

7 Post conditions

None

8 Business Rules

Security

- There are four types of users available within eHEAT System.
  - eHEAT Admin
  - DOC User (DOC & State Fiscal users)
  - Service Provider Admin
  - Vendor Admin

- eHEAT admin user has access to all these screens, and allowed to perform the following tasks for user types DOC User, Service Provider Admin and Vendor Admin:
  - Creating new user
  - Editing existing user
  - Resetting password for the user
  - Disabling existing user
  - Enabling already disabled user
  - Creating new role
  - Editing existing role
  - Deleting existing role
  - Assign functions to role

- Service Provider admin and Vendor admin can also perform the above-specified functions for their organization users. Service provider admin and Vendor admin are not allowed to manipulate/view other organizations users and roles details.

- All other users have access to the “Change Password” screen.

- System by default will have two eHEAT admin users called “admin” and “batch”. Batch user id will be used for batch processes.

Terms

- A user is the individual representing an eHEAT actor
- A group is a named collection of users who will involve in the activity of eHEAT System. The group is the actor defined by the use case documents. The Group is also tied to a master list of all the functions defined in the use cases for a particular actor.
- A role is a named collection functions in the eHEAT System
- A function is a set of functionality defined for scenarios in the use cases for an actor

Manage User

- A user can belong to only one group.
- Once a user has been assigned to a group, the group cannot be modified.

- Once a user has been assigned with a type, the user type cannot be modified.
- A user can be assigned to multiple roles. The role associated with the user can be modified at any time.
- Once a user has been created, the user id can not be modified.

Manage Role a

- A user role can belong to only one group.
- Group assigned for a role can be modified only if the role is not associated with any user.
- One or more System functions can be assigned to a user role.
- Manage Role function is allowed only for users with type eHEAT admin, Service Provider Admin and Vendor Admin
- eHEAT admin users can manipulate roles for users with types DOC User, Service Provider Admin and Vendor Admin.
- Service Provider admin can create roles for their organization users only.
- Vendor admin can create roles for their organization users only.
- A user role will not be allowed to delete if the role is associated with users.
- System will not allow to the user to create duplicate role names.

Change password

- Logged in user can change his/her own password by providing valid old password, new password and confirm password.
- New password cannot be same as old password.

Design Considerations

- A detailed design of user security will be performed where more business rules might be discovered by taking into account the details described in the use case documents.
- Data Security requirements are described in the use cases. These will be incorporated into the security design during the technical design stage.