Privilege Management and Enforcement System (PMES)

Project Plan

SW3460

SOFTWARE METHODOLOGY

Prof. Shing

December 27, 2004

(Final)

Jack Chung
Jeff Gorsch
Cop Le

Introduction:

This project plan specifies the scope of effort necessary to design, develop, and test the Privilege Management and Enforcement System (PMES) for Prof. Man-Tak Shing in accordance with "SW3460 Software Methodology Term Project," ref. A. It includes sections for project description, deliverables, project assumptions and risks, project organization, schedule, quality plan, test plan, documentation plan, technical reviews, technical information, and applicable documents.

Project Description:

PMES is a distributed resource-sharing environment that provides privilege management and enforcement features. It is an enabler for effective collaboration between autonomous organizations that wish to work as one. Although existing business-to-business (B2B) applications and services can address some of the needs of such businesses, they do not currently provide a sufficiently secure or scalable environment for dynamic, internet-based collaboration. PMES will allow seamless integration of dynamically allocable resources across multiple organizations and through multiple access methods. It will facilitate flexible yet secure protocols for allocating resource privileges within and between enterprises. And it will provide powerful administrative and management tools via a web-based interface. Privilege and enforcement options include user and group rights (read, write, change, execute, admin), time-based access, and interdependency and/or mutual exclusion. Users will also be able to delegate privilege management to another enterprise when the local network is unavailable. Resource rights are strictly enforced, security rules are applied to provide early warning of potential security problems, and all unauthorized access attempts are logged. In general, users for this system will include managers, employees, business partners, associates, contractors, and system administrators for enterprise businesses utilizing the Internet. Specifically, users will include people who are required to gather information before conducting business transactions, or manage business on local or remote sites. Users must be capable of connecting to the Internet via computer terminal, laptop, or wireless handheld device.

Deliverables:

- Team Roster [4 OCT 04]
- Project Plan [18 OCT 04]
- Requirements Document [1 NOV 04]
- Design Document [22 NOV 04]
- Code, Test Plans, Test Results [27 DEC 04]
- Installation/User Manual [27 DEC 04]
- Lessons Learned [27 DEC 04]
- Team Assessment [27 DEC 04]

Project Assumptions and Risks:

Assumptions – Current scheduling reflects consistent availability of resources, including personnel, equipment, and third-party software products.

Risks – Potential problems include unexpected travel of team members, equipment failure or unavailability, and an unexpectedly steep learning curve for required software tools. These risks will be mitigated via regular team meetings, rotating task assignments, and proactive planning of resource use.

Project Organization (Team Roster):

Task assignments will be split and rotated between all team members (listed below):

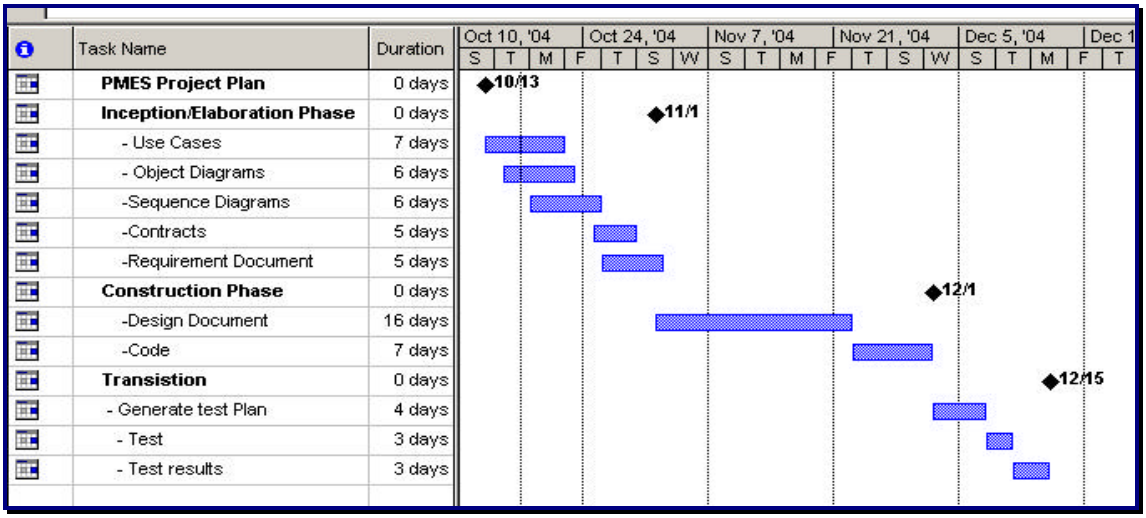
Jack Chung,
Jeff Gorsch,
Cop Le

Schedule:

Phases of Development -- The Unified Process will be used for the design and development of this system providing for iterative and incremental development.

Phase 1, Inception and Elaboration:	Define Scope, Generate Requirements, and Develop Architectural Prototype
Phase 2, Construction:	Develop System Prototype
Phase 3, Transition:	Test System Prototype, Generate and Install User Manual

Milestones -- Microsoft Project™ will be used to track the progress of the design, development and testing of this project.



Quality Plan:

Change Control – Changes in project scope will be agreed upon by unanimous consent of all team members.

Configuration Management – All deliverables will be assigned a revision date. Preliminary document deliverables will be marked "Draft." Submitted document deliverables will be marked "Final." All draft document deliverables will be reviewed by available team members and, if possible, submitted to the customer before final review. Software products will be assigned a version number corresponding to major build (which will be 0 for Beta versions) followed by an increment for minor builds, i.e. version 0.1 or 1.0.

Release Control – Software coding, validation, and verification will be split among all three team members, with each providing quality assurance review of the others' work products. Software will be released upon unanimous consent.

Test Plan:

The Software Test Plan is provided as a separate deliverable.

Documentation Plan:

Documentation will take the form of a one-page user/installation manual, and will be completed per the master schedule.

Technical Reviews:

Technical reviews will be performed concurrently with weekly team meetings.

Technical Information:

The following development tools will be used for software production –

Macromedia Dreamweaver™ and/or Borland Delphi.™

Applicable Documents:

Ref. A -- "SW3460 Software Methodology Term Project," Shing, Man-Tak, 2004.

Privilege Management and Enforcement System (PMES)

System Requirements Document

SW3460

SOFTWARE METHODOLOGY

Prof. Shing

December 27, 2004

(Final)

Jack Chung
Jeff Gorsch
Cop Le

Privilege Management and Enforcement System (PMES) (System Requirements Document)

Table of Contents

REVISION SHEET

Revision Number	Date	Brief summary of changes
1	11/1/04	Remove resource database use case
2	11/14/04	Modified specification requirements.
3	11/28/04	Modified sequence diagram and use cases.

1. Introduction

1.1 Purpose

This document details the functional and non-functional requirements for the "Privilege Management and Enforcement System" (PMES).

1.2 Scope

This document defines the software requirements of the PMES. Hardware requirements are not directly addressed. The system, and any locally required software components, will be accessible on the Internet via web browser. The product will be created with Macromedia Dreamweaver™ and will interface with an SQL-based enterprise resource database.

1.3 Objectives and success criteria of the project

Iterative evaluations will be conducted of the concepts and prototypes developed. The goal of this process is to estimate the performance and usability of the system. The following types of evaluation will be used:

a) *Qualitative Evaluation:* Through analysis of the requirements and relative merits of our proposal, we intend to evaluate the feasability of such a system by conducting research to determine expected performance in each stage of devolpment. Further, a review of system performance will be conducted against the requirements document prior to project completion.

b) *Simulation:* Team members will use Dreamweaver to develop a model of the PMES. This model will be updated to reflect current design at each stage of development.

c) *Usability:* Team members will solicit usability recommendations from potential users prior to the construction of the prototype via user surveys.

1.4 Definitions, acronyms, and abbreviations

A complete glossary of terms, definitions, acronyms, and abbreviations has been provided in section 4 of this document.

1.5 References

[1] IEEE Std 830-1998 "Recommended Practice for Software Requirements Specifications."

[2] IEEE Std 1233-1998 "Guide for Developing System Requirements Specifications."

[3] IEEE Std 1016-1998 “Recommended Practice for Software Design Descriptions.”

[4] ISO Std 9126 “Software Quality.”

2. Current System

Current Business-to-Business (B2B) enterprise solutions do not provide a sufficiently secure or scalable environment for dynamic, internet-based collaboration. Those systems that do exist lack uniformity and have time-consuming and inefficient configuration requirements. This leads to high costs and potential security vulnerabilities. This is unacceptable in an increasingly volatile and complex operating environment.

3. Proposed System

Our proposed solution is a dynamic, web-based privilege management and enforcement interface that enables independent enterprises to seamlessly manage network security across the web. Users with Internet access (via computer terminals, laptops, wireless computers, etc.) can log on to the system website to access enterprise services and resources. PMES enables enterprises to manage local resources by setting privileges that users must have for legal access, and grant remote privileges for users to access resources in other enterprises. The system is designed to meet today’s web-based enterprise management and service needs.

3.1 Overview

The goal is to allow easy access to web-based resources for enterprise service users. The system will utilize existing web-based infrastructure and technology to provide users a single place in the web to obtain web-based services. The website can be accessed through wired or wireless computer terminals, laptops, or handheld computers. Fault tolerance is provided through the ability to delegate privileges to another enterprise in the event of local system failure or required maintenance.

3.2 Functional Requirements

A. User Login and Authentication -- PMES will enable access through a standard web-based user login procedure. Users will be prompted for a username and password in order to access website contents.

B. Resource Access -- PMES will allow users with the proper credentials to read web contents, upload, download, modify, and execute files, and to access network services (print servers, databases, etc.) and the local help system.

C. New User Account Creation -- PMES will allow the system administrator to create new user accounts via web-based form entry.

D. User Privilege Assignment -- PMES will allow the assignment of the following user access rights:

    a. Read, write, execute, admin, and delete (files).
    b. Use (network services).
    c. Time-based access (strictly enforced).
    d. Interdependency and/or mutual exclusion relationships.
    e. Remote resource access via “privilege certificates.”

E. System / User Monitoring -- PMES will allow the system administrator to conduct background monitoring of system and user activities. All user activity and entry attempts will be recorded and available for review. Administrators will be alerted if access patterns matching the rules in its security alert database are detected.

F. Authority Delegation -- PMES will allow the system administrator to delegate authority to local users for the purposes of decentralized control and fault tolerance. Control can be ceded to a remote system administrator under the following conditions:

    a. Loss of local Internet connectivity.
    b. Local network failure.
    c. Local network maintenance.

G. Troubleshooting: PMES will allow the system administrator to troubleshoot any network and/or software related issues.

3.3 Nonfunctional Requirements

3.3.1 Security

PMES will implement the Open Software Foundation's Distributed Computing Environment (DCE) and Distributed File System (DFS) as a means for system security.

3.3.2 Usability

Although the PMES is designed with all current best-practices in mind, it is ultimately the end user that determines usability. Thus, the primary usability objectives will be evaluated via user surveys to be conducted following production of the prototype.

Initial usability requirements include:

A. Simplicity of Design: Web pages will minimize the number and complexity of components necessary to provide needed information, minimize the number of mouse clicks necessary to navigate to a desired page, and minimize the size of graphical elements to provide fast page loads.

B. Variable Frame Size: Web pages will support variable display sizes to accommodate portability between platforms.

C. Familiar Interface: Web pages will use standard web page features, including main menus, a navigation frame, consistent text layout using Cascading-Style Sheets (CSS), and consistent navigational tools (home, index, help).

D. Accessibility: Web pages will be designed for accessibility to the disabled.

E. Help System: PMES will provide a full-featured, indexed help system.

F. Error Notices: All system faults will result in plainly written, English language notifications and include a link to the PMES help system.

3.3.3 Reliability

A. Fatal system errors, resulting in system downtime, will have a mean time between failures of at least 1000 hours.

B. Fatal System errors will exit the user out of the web site and not interrupt Internet access.

C. Security and virus attacks that meet predetermined thresholds will result in immediately shut down of the infected website and an automatic switch to an alternate website within 5 minutes.

3.3.4 Performance

A. The system will be designed to accommodate 100 simultaneous transactions.
B. The system should respond to each user input within 10 seconds.

3.3.5 Supportability

A. The system will be developed in Dreamweaver and run on any platform that supports standard web servers.
B. The system requires that each user have Internet access.

3.3.6 Implementation

The system will be implemented using Dreamweaver/ASP and an SQL database.

3.3.7 Interface

The system will utilize XHTML 1.0 via the World-Wide Web (WWW).

User Configuration

Any needed system components or system configuration will be available for electronic transfer via the WWW.

3.3.8 Legal

Supporting documentation for this system will include an end-user license agreement (EULA) that limits liability for the developers of the PMES.

3.4 System Models

3.4.1 Scenarios

General Operational Scenario:

The user turns on a wireless or fixed-wire computing device with Internet access. When connected to the Internet, the user accesses www.pmes.com. The user enters a valid user name and password and is granted access. The user accesses enterprise resources, exchanges business information, and works collaboratively with a remote business partner. The user completes work and logs off the system.

3.4.2 Use case model

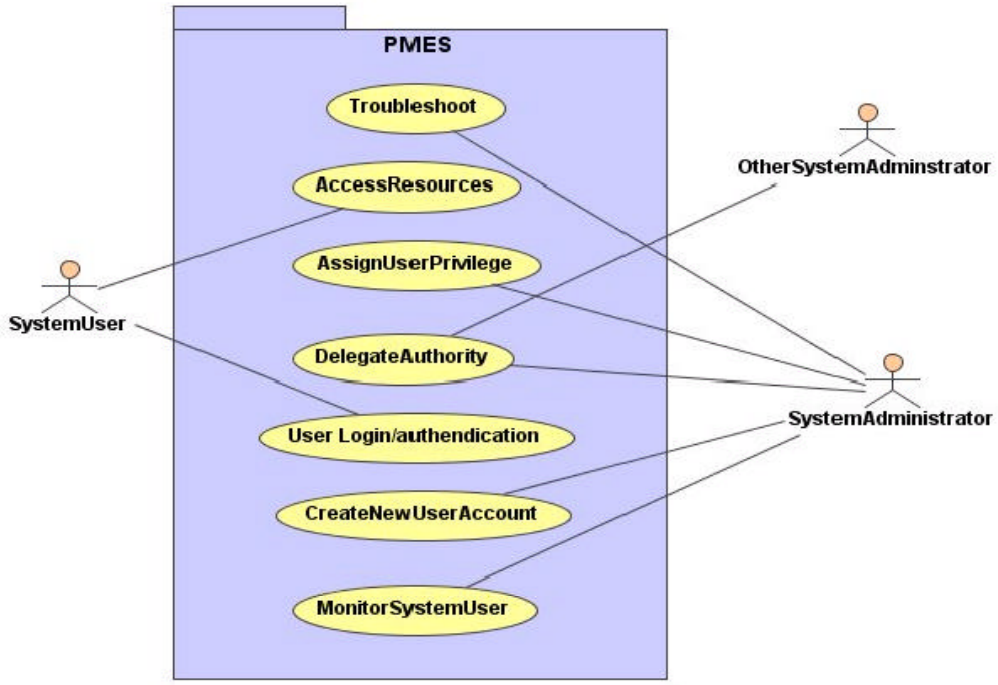


Figure (1)

Use case: UC-1 User Login and Authentication

Primary Actor: System User

Flow of Events:

1. The System User accesses the PMES website and clicks the "Login' link.
2. PMES prompts the System User for User Name and Password.
3. The System User enters a valid User Name and Password and clicks the "Login" button.
4. PMES authenticates the System User, initiates the User Log, and displays the main system page.

Entry condition: The System User has Internet access.

Exit condition: The System User is successfully logged into the PMES website.

Exceptions:

1a. PMES advises the System User that PMES requires the System User's web browser to accept "cookies" and displays a Help screen.

4a. The System User is disconnected from PMES due to service problems.

Quality requirements:

- The System User will be automatically Logged-Out after 15 minutes of inactivity.
- PMES will lock-out a user account for 24 hours if an invalid username or password has been entered three times.

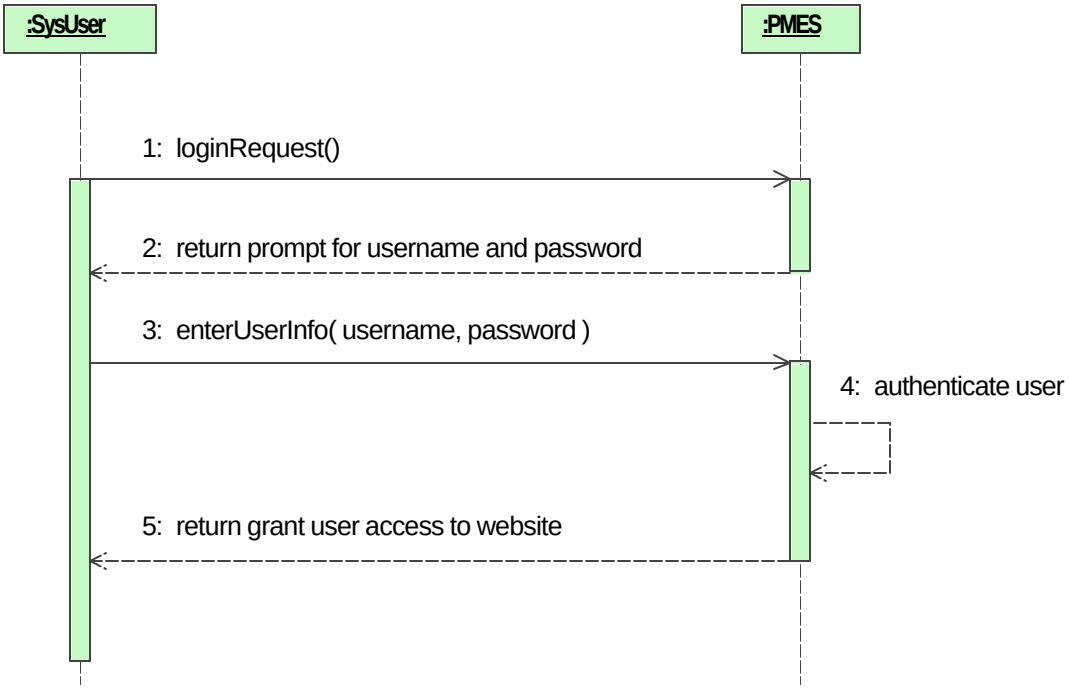


Figure (2)

Note: For initial prototyping requirements, the loginRequest function is considered to have trivial post-conditions. An Operation Contract will therefore not be provided at this time.

Contract: C1 – Enter User Information
Operation: enterUserInfo()
Cross Ref: UC 1 – User Login and Authentication

Preconditions:

1. An instance ***w*** of Website has been created.
2. The User has successfully connected to the Internet.
3. An instance ***ul*** of UserList has been created.

Post-conditions:

1. A new instance ***u*** of User was created.
2. ***u*** was associated with ***w*** (via the "login" association).
3. ***u*** was associated with ***ul*** (via the "in" association).

Use case: UC-2 Access Resources

Primary Actor: System User

Flow of Events:

1. The System User logs into the PMES website (UC-1) and clicks the "Resources" link.
2. PMES displays a page with a list of available resources (the Resource Page).
3. The System User selects an available resource by clicking on the resource name and then clicks the "Download" button.
4. PMES downloads the selected resource, adds the action to the User Log, and displays a prompt confirming the download.
5. The System User clicks the "OK" button.
6. PMES returns the System User to the Resource Page.
7. The System User modifies the resource on his local computer, clicks on the previously selected resource name, and then clicks the "Replace" button.
8. PMES uploads the modified resource, adds the action to the User Log, and displays a prompt confirming the upload and resource replacement.
9. The System User clicks the "OK" button.
10. PMES returns the System User to the Resource Page.
11. The System User clicks on the previously selected resource name and then clicks the "Print" button.
12. PMES sends the resource to the selected printer, adds the action to the User Log, and displays a prompt confirming the action performed.
13. The System User clicks the "OK" button.
14. PMES returns the System User to the Resource Page.

Entry condition: The System User has Internet access.

Exit condition: The System User has successfully accessed PMES resources.

Exceptions: 4a, 8a, 12a. A system / network error prevents access to the selected resource; an alert is displayed to the System User.

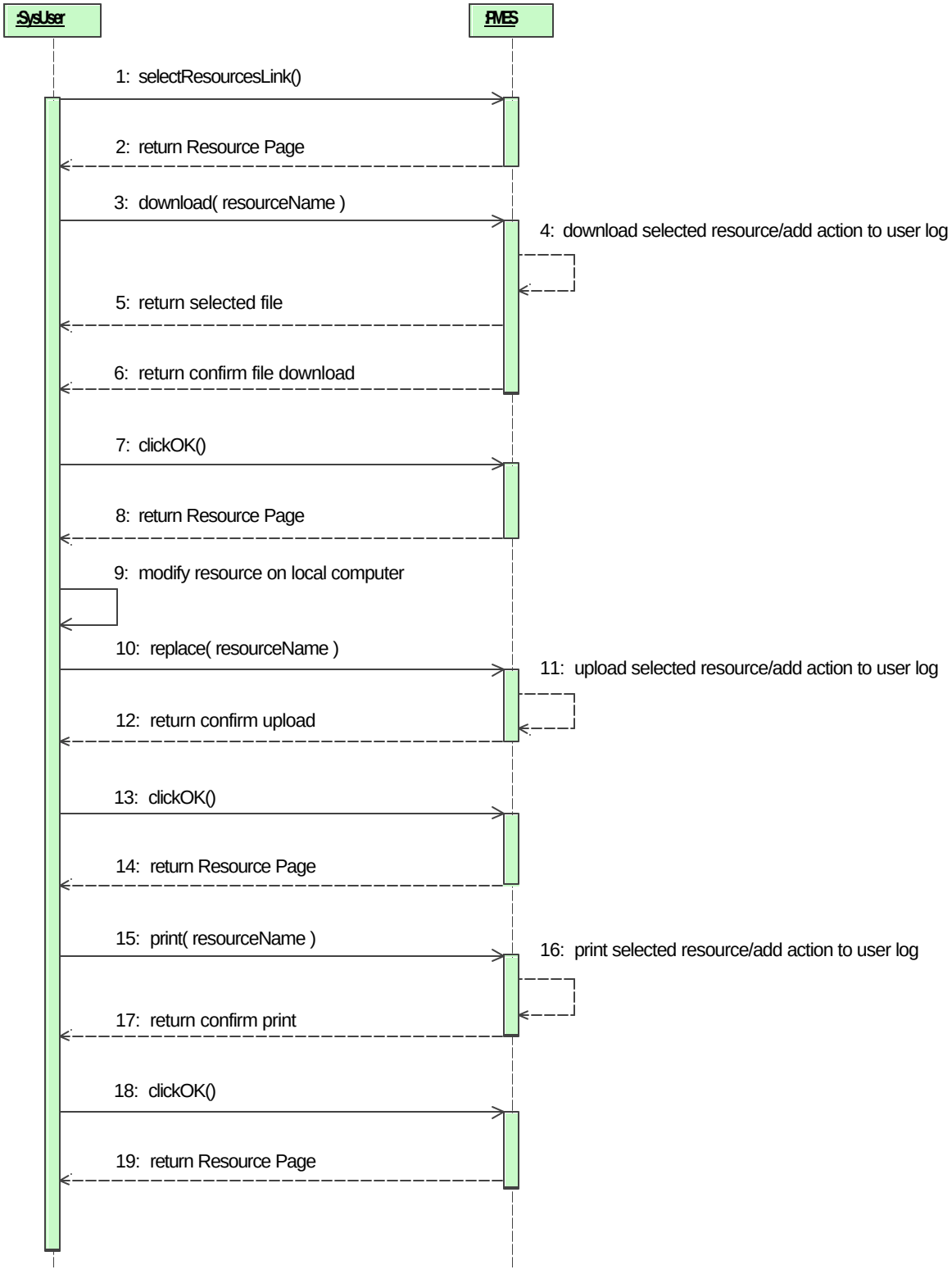

:SysUser
:PMES
1: selectResourcesLink()
2: return Resource Page
3: download(resourceName)
4: download selected resource/add action to user log
5: return selected file
6: return confirm file download
7: clickOK()
8: return Resource Page
9: modify resource on local computer
10: replace(resourceName)
11: upload selected resource/add action to user log
12: return confirm upload
13: clickOK()
14: return Resource Page
15: print(resourceName)
16: print selected resource/add action to user log
17: return confirm print
18: clickOK()
19: return Resource Page

Figure (3)

Note: For initial prototyping requirements, the selectResourceLink and the clickOK functions are considered to have trivial post-conditions. Operation Contracts will therefore not be provided at this time.

Contract: C2 – Download Resource
Operation: download(resourceName)
Cross Ref: UC 3 – Access Resource

Preconditions:

1. An instance ***w*** of Website has been created.
2. The System User has successfully logged-in to the PMES website.
3. An instance ***u*** of User has been created.

Post -conditions:

1. An instance ***r1*** of Resource was created.
2. ***r1*** was associated with ***u*** (via the "download" association).

Contract: C3 – Replace Resource
Operation: replace(resourceName)
Cross Ref: UC 3 – Access Resource

Preconditions:

1. An instance ***w*** of Website has been created.
2. The System User has successfully logged-in to the PMES website.
3. An instance ***r1*** of Resource has been created.
4. An instance ***u*** of User has been created.

Post -conditions:

1. An instance ***r2*** of Resource was created.
2. Instance ***r1*** of Resource was destroyed.
3. An instance ***u*** of the "upload" association was created between ***w*** and ***r2***.
4. ***r2*** was associated with ***u*** (via the "upload" association).

Contract: C4 – Print Resource
Operation: print(resourceName)
Cross Ref: UC 3 – Access Resource

Preconditions:

1. An instance ***w*** of Website has been created.
2. The System User has successfully logged-in to the PMES website.
3. An instance ***r2*** of Resource has been created.
4. An instance ***u*** of User has been created.

Post -conditions:

1. ***r2*** was associated with ***u*** (via the "print" association).

Use case: UC-3 Create New User Account

Primary Actor: System Administrator

Flow of Events:

1. The System Administrator logs into the PMES website (UC-1).
2. PMES automatically displays menu items appropriate for a user with administrative privileges.
3. The System Administrator selects the "Users" link.
4. PMES displays the Current Users page.
5. The System Administrator clicks on the "Create" button below the Users List.
6. PMES displays a "New User" form with entries for User Name and Initial Password, and a list of available privileges.
7. The System Administrator enters data for the appropriate fields in the "New User" form, selects a privilege level, and clicks the "OK" button.
8. PMES creates a new user account, assigns the selected privilege level, adds the user data to the System Database, initiates the User Log, displays the **"**New User Created**"** prompt, and records the corresponding actions in the System Log.
9. PMES sends an e-mail notification to the selected user to inform them of their newly created user account, displays the "E-mail notification sent" prompt, and records the action in the System Log.
10. The System Administrator responds by clicking the "OK" button.
11. PMES returns the System Administrator to the Current Users page.

Entry condition: The System Administrator has Internet access.

Exit condition: The System Administrator has successfully created a new user account.

Exceptions:

8a. A system / network error prevents changes to the System Database; the System Administrator is informed of the error.

9a. A system / network error prevents e-mail notification; the System Administrator is informed of the error.

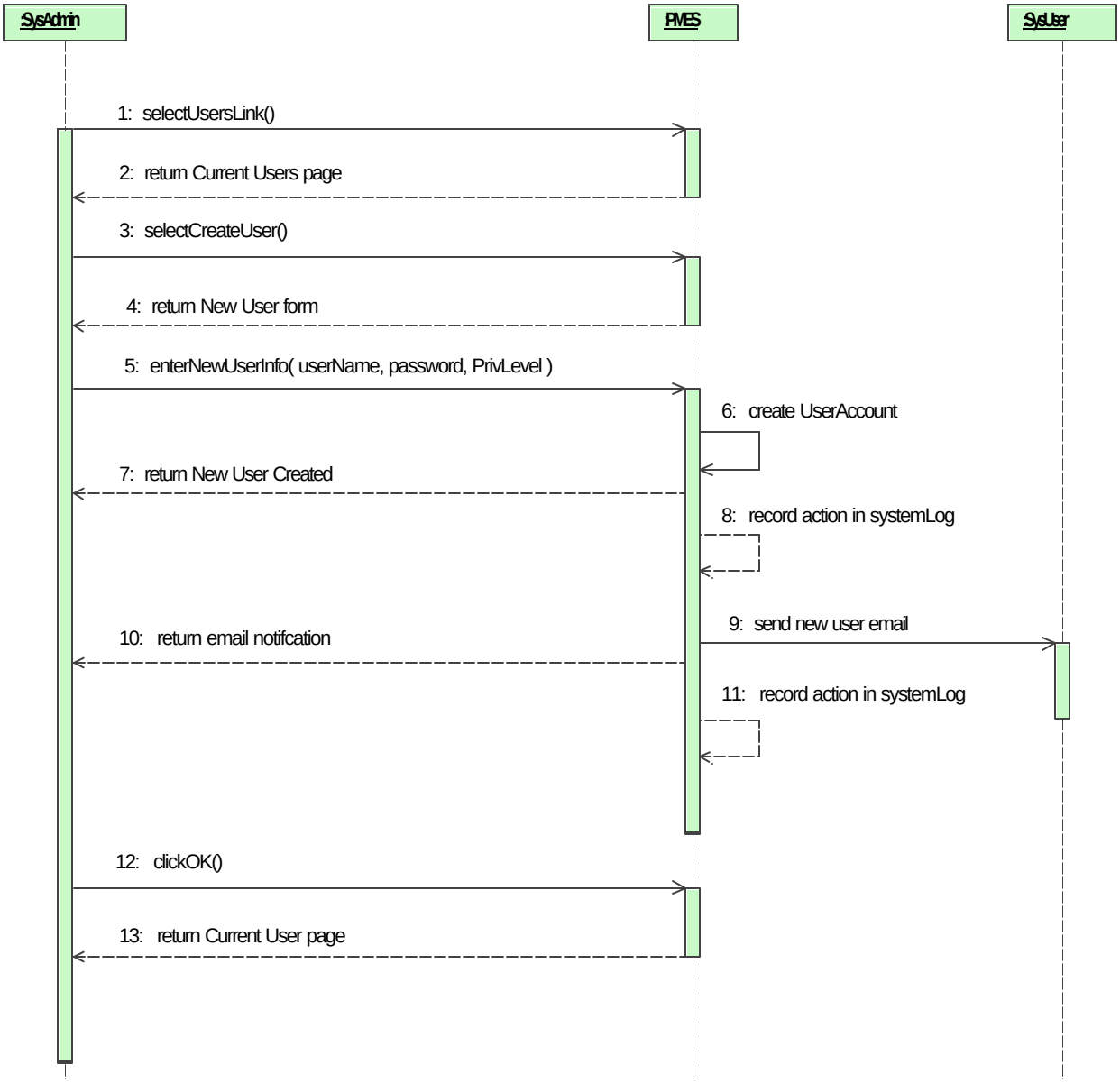

SysAdmin
PMES
SysUser
1: selectUsersLink()
2: return Current Users page
3: selectCreateUser()
4: return New User form
5: enterNewUserInfo(userName, password, PrivLevel)
6: create UserAccount
7: return New User Created
8: record action in systemLog
9: send new user email
10: return email notifcation
11: record action in systemLog
12: clickOK()
13: return Current User page

Figure (4)

Note: For initial prototyping requirements, the selectUsersLink, selectCreateUser, and clickOK functions are considered to have trivial post-conditions. Operation Contracts will therefore not be provided at this time.

Contract: C5 – Enter New User Information
Operation: enterNewUserInfo()
Cross Ref: UC 3 – Create New User Account

Preconditions:

1. An instance ***w*** of Website has been created.
2. The System Administrator has successfully logged-in to the PMES website.
3. An instance ***sa*** of SysAdmin has been created.

Post -conditions:

1. A new instance ***ua*** of UserAccount was created.
2. ***ua*** was associated with ***sa*** (via the "create" association).
3. The UserName property of ***ua*** was set to NewUserForm.UserName.
4. The Password property of ***ua*** was set to NewUserForm.Password.
5. The PrivLevel property of ***ua*** was set to NewUserForm.PrivLevel.
6. An instance ***ule*** of UserLogEntry was created.
7. ***ule*** was associated with ***w*** (via the "create" association).

Use case: UC-4 Assign User Privilege

Primary Actor: System Administrator

Flow of Events:

1. The System Administrator logs into the PMES website (UC-1).
2. PMES automatically displays menu items appropriate for a user with administrative privileges.
3. The System Administrator selects the "Users" link.
4. PMES displays the Current Users page.
5. The System Administrator selects the name of the user for which privileges are to be assigned and clicks the "Privileges" button.
6. PMES displays a list of current privileges for the selected user and a list of privileges available to be assigned.
7. The System Administrator selects the desired new privileges and clicks the "OK" button.
6. PMES displays the **"**Confirm privilege assignment**"** prompt to confirm the previous selection.
7. The System Administrator responds by clicking the "OK" button.
8. PMES grants the selected privileges to the appropriate user, displays the **"**privilege(s) granted**"** prompt, and records the action in the System Log.
9. PMES sends an e-mail notification to the selected user to inform them of their newly assigned privileges, displays the "E-mail notification sent" prompt, and records the action in the System Log.
10. The System Administrator responds by clicking the "OK" button.
11. PMES returns the System Administrator to the Current Users page.

Entry condition: The System Administrator has Internet access.

Exit condition: The System Administrator has successfully assigned new user privileges.

Exceptions: 7a, 8a. A system / network error prevents (changes to the System Database / e-mail notification); the System Administrator is informed of the error.

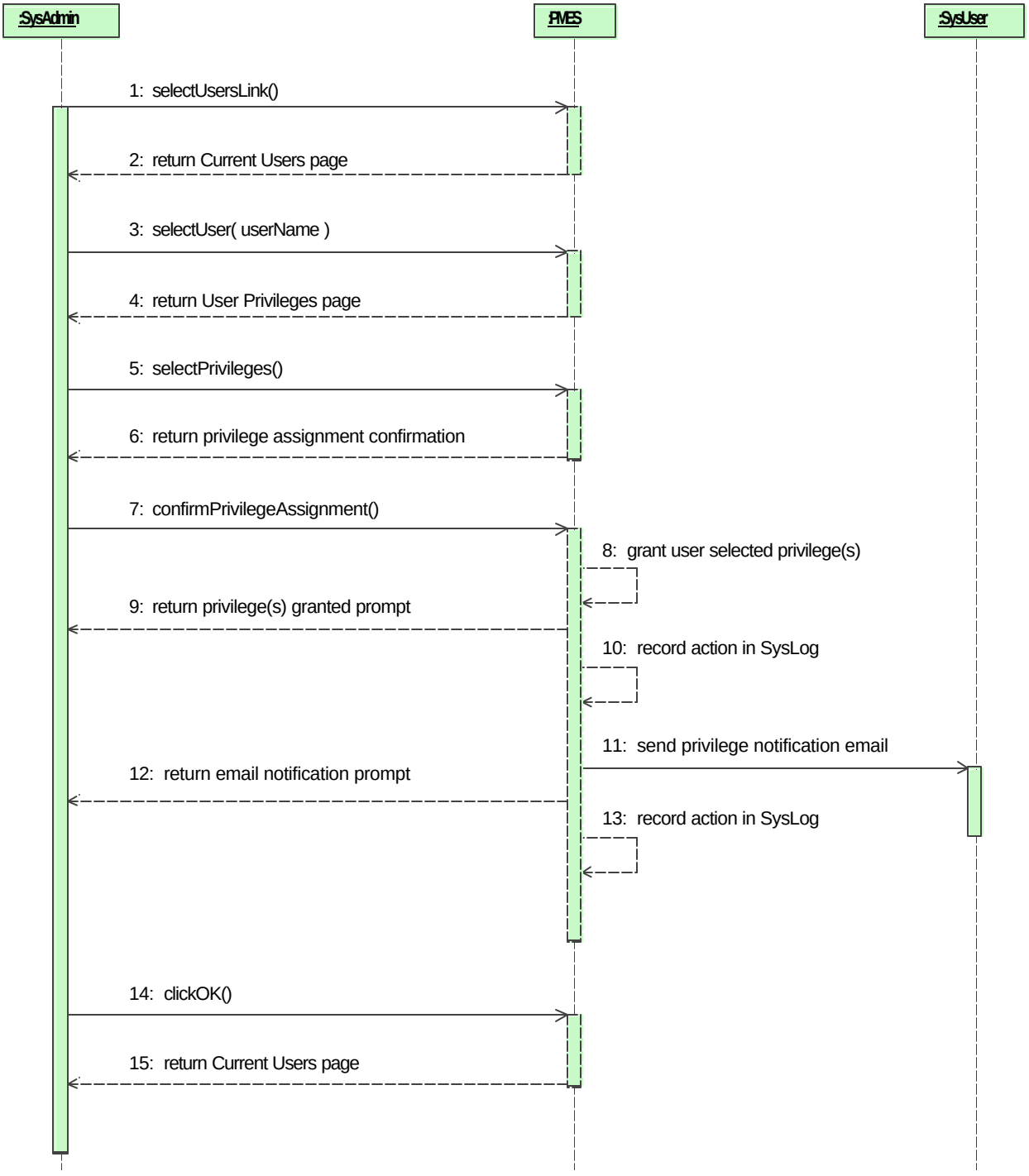

:SysAdmin
:PMES
:SysUser
1: selectUsersLink()
2: return Current Users page
3: selectUser(userName)
4: return User Privileges page
5: selectPrivileges()
6: return privilege assignment confirmation
7: confirmPrivilegeAssignment()
8: grant user selected privilege(s)
9: return privilege(s) granted prompt
10: record action in SysLog
11: send privilege notification email
12: return email notification prompt
13: record action in SysLog
14: clickOK()
15: return Current Users page

Figure (5)

Note: For initial prototyping requirements, the selectUsersLink and the clickOK functions are considered to have trivial post-conditions. Operation Contracts will therefore not be provided at this time.

Contract: C6 Select User
Operation: selectUser(userName)
Cross Ref: UC 4 – Assign User Privilege

Preconditions:

1. An instance ***w*** of Website has been created.
2. The System Administrator has successfully logged-in to the PMES website.
3. An instance ***sa*** of SysAdmin has been created.

Post -conditions:

1. An instance ***ua*** of UserAcount was created.
2. The attributes of ***ua*** were initiated.
3. An instance ***pl*** of PrivilegeList was created.
4. The attributes of ***pl*** were initiated.
5. ***pl*** was associated with ***ua***.
6. Current and available privileges are returned to the caller.

Contract: C7 Confirm Privilege Assignment
Operation: confirmPrivilegeAssignment()
Cross Ref: UC 4 – Assign User Privilege

Preconditions:

1. An instance ***w*** of Website has been created.
2. The System Administrator has successfully logged-in to the PMES website.
3. An instance ***sa*** of SysAdmin has been created.
4. An instance ***ua*** of UserAcount has been created.
5. An instance ***pl*** of PrivList has been created.

Post -conditions:

1. One or more instances p_n of Privilege were created.
2. Each instance p_n was associated with ***pl***.
3. An instance ***sle*** of SysLogEntry was created.
4. ***sle*** was associated with ***w*** (via the "create" association).
5. System actions were added to ***sle***.

Use case: UC-5 Monitor Website

Primary Actor: System Administrator

Other Actors: System Users

Flow of Events:

1. The System Administrator logs into the PMES website (UC-1).
2. PMES automatically displays menu items appropriate for a user with administrative privileges.
3. The System Administrator selects the "Monitor" link.
4. PMES displays a monitoring page with a list of current users and their activities; the system highlights any unusual or suspicious activity with a color code (yellow or red, depending on severity level) and displays a list of advisories / warnings under the "Current Users" list.

Entry condition: The System Administrator has Internet access.

Exit condition: The System Administrator has successfully monitored user activity.

Exceptions:

a. The System Administrator detects suspicious activity, selects the appropriate user(s) in the Current Users list, the clicks the "Suspend" button.
b. PMES suspends the user account of the selected user(s), logs-out the selected user(s), and notifies the effected user(s) that their user account has been suspended.

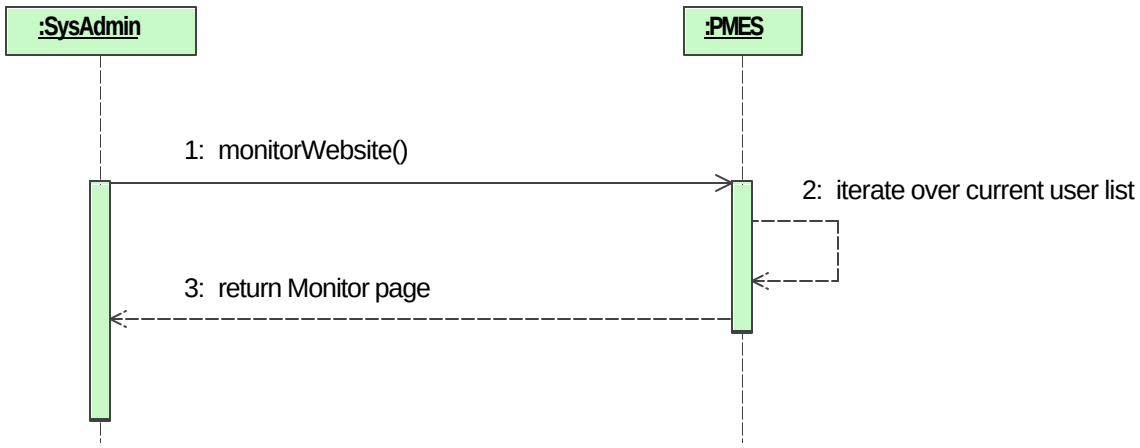


Figure (6)

Contract: C8 – Monitor Website
Operation: monitorWebsite()
Cross Ref: UC 5 – Monitor Website

Preconditions:

1. An instance ***w*** of Website has been created.
2. The System Administrator has successfully logged-in to the PMES website.
3. An instance ***sa*** of SysAdmin has been created.
4. An instance ***ul*** of UserList has been created.

Post -conditions:

1. ***sa*** was associated with ***w*** (via the "monitor" association).
2. A list of current users (from ***ul***) is returned to the caller.
3. A list of current user activities is returned to the caller.

Use case: UC-6 Delegate Authority

Primary Actor: System Administrator

Other Actors: Assistant / Alternate System Administrator

Flow of Events:

1. The System Administrator logs into the PMES website.
2. PMES automatically displays menu items appropriate for a user with administrative privileges.
3. The System Administrator selects the "Delegate" link.
4. PMES displays the "Delegate Authority" form.
5. The System Administrator selects assistant / alternate system administrator(s) from the "System Users" list, an appropriate authority level from the "Privileges" list, and clicks the "OK" button.
6. PMES displays the **"**Confirm delegation of authority**"** prompt to confirm the previous selection.
7. The System Administrator responds by clicking the "OK" button.
8. PMES grants the selected privileges to the appropriate user(s), displays the **"**Delegation granted**"** prompt, and records the action in the System Log.
9. PMES sends an e-mail notification to the selected user(s) to inform them of their newly assigned privileges, displays the "E-mail notification(s) sent" prompt, and records the action in the System Log.
10. The System Administrator responds by clicking the "OK" button.
11. PMES returns the System Administrator to the Main page.

Entry condition: The System Administrator has Internet access.

Exit condition: Authority selected by the System Administrator is delegated to the assigned user(s).

Exceptions: 8a, 9a. A system / network error prevents (changes to the System Database / e-mail notification); the System Administrator is informed of the error.

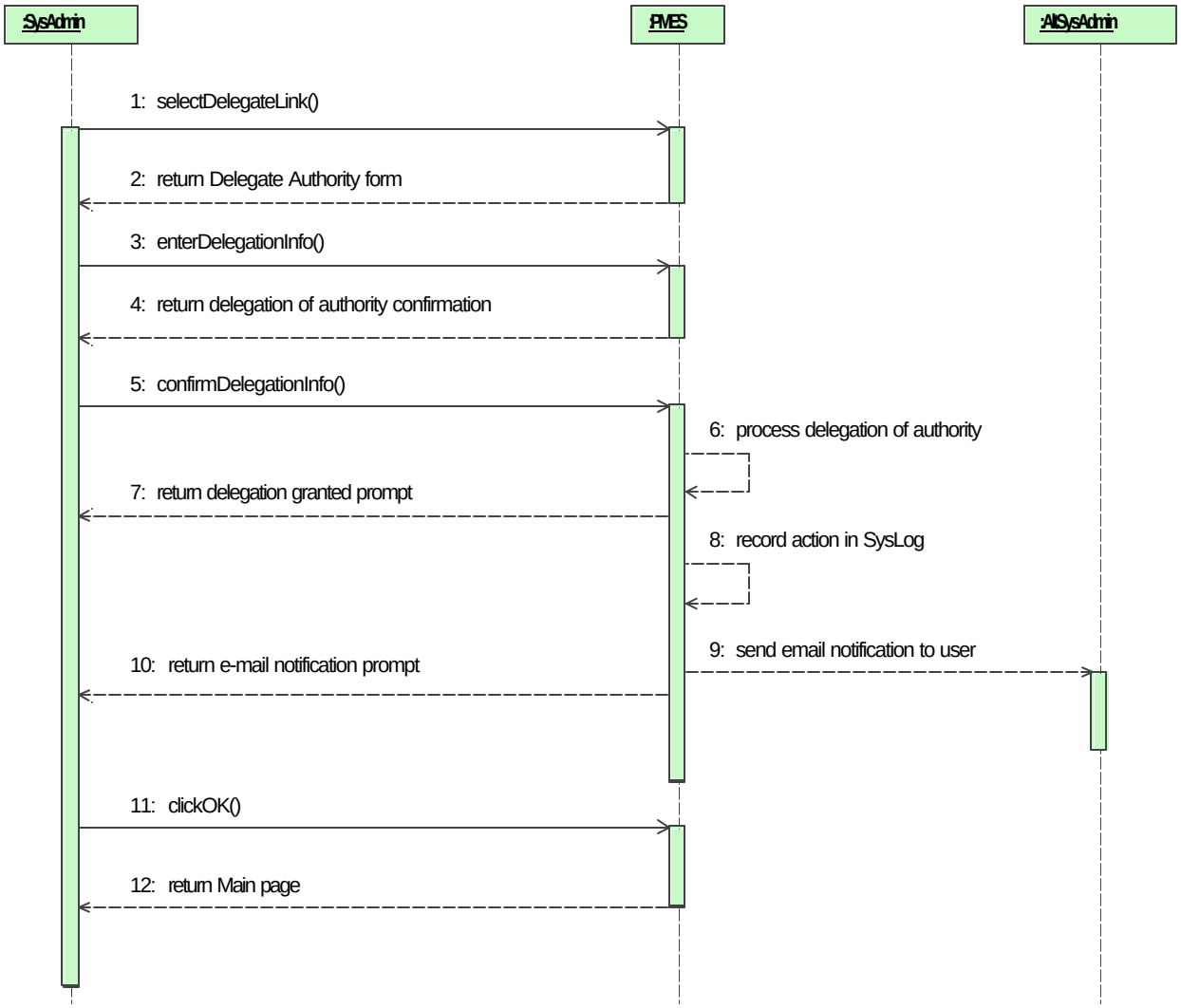

:SysAdmin
:PMES
:AllSysAdmin
1: selectDelegateLink()
2: return Delegate Authority form
3: enterDelegationInfo()
4: return delegation of authority confirmation
5: confirmDelegationInfo()
6: process delegation of authority
7: return delegation granted prompt
8: record action in SysLog
9: send email notification to user
10: return e-mail notification prompt
11: clickOK()
12: return Main page

Figure (7)

Contract: C9 Enter Delegation Information
Operation: enterDelegationInfo()
Cross Ref: UC – 6 Delegate Authority

Preconditions:

1. An instance ***w*** of Website has been created.
2. The System Administrator has successfully logged-in to the PMES website.
3. An instance ***sa*** of SysAdmin has been created.

Post -conditions:

1. An instance ***ua*** of UserAcount was created.
2. An instance ***pl*** of PrivList was created and associated with ***ua***.

Contract: C10 Confirm Delegation Information
Operation: confirmDelegationInfo ()
Cross Ref: UC – 6 Delegate Authority

Preconditions:

1. An instance ***w*** of Website has been created.
2. The System Administrator has successfully logged-in to the PMES website.
3. An instance ***sa*** of SysAdmin has been created.
4. An instance ***ua*** of UserAcount has been created.
5. An instance ***pl*** of PrivList has been created and associated with ***ua***.
6. An instance ***sl*** of SysLog has been created.

Post -conditions:

1. New privileges were assigned to ***pl***.
2. An instance ***sle*** of SysLogEntry was created.
3. System actions were added to ***sle***.
4. ***sle*** was associated with ***sl***.

Use case: UC-7 Troubleshoot

Primary Actor: System Administrator

Flow of Events:

1. The System Administrator logs into the PMES website (UC-1).
2. PMES automatically displays menu items appropriate for a user with administrative privileges.
3. The System Administrator selects the "Troubleshoot" link.
4. PMES displays a "Troubleshooting" page with a list of current system faults, highlights faults with a color code (yellow or red, depending on severity level), displays a list of advisories / warnings under the "System Faults" list, and provides appropriate links to the Help system.

Entry condition: The System User has Internet access.

Exit condition: The System Administrator has successfully reviewed the troubleshooting information provided by PMES.

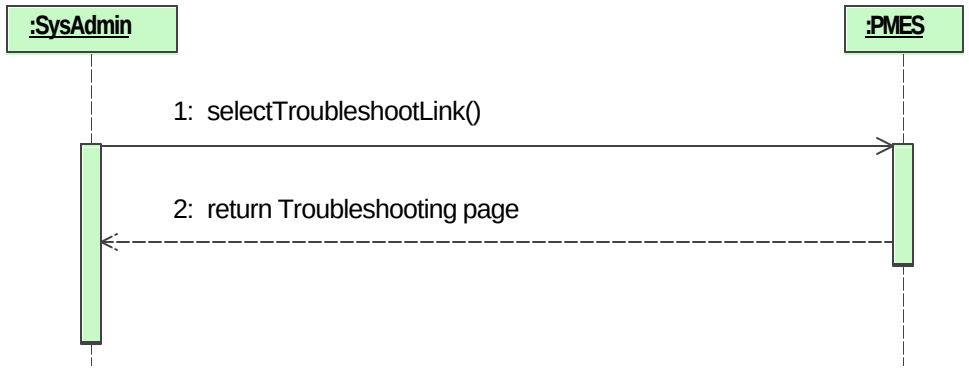


Figure (8)

Contract: C11 Select Troubleshoot
Operation: selectTroubleshoot()
Cross Ref: UC 7 – Troubleshoot

Preconditions:

1. An instance ***w*** of Website has been created.
2. The System Administrator has successfully logged-in to the PMES website.
3. An instance ***sa*** of SysAdmin has been created.

Post -conditions:

1. For each fault detected, an instance f_n of SysFault was created and associated with ***w*** and ***sa***.

3.4.3 Conceptual Model

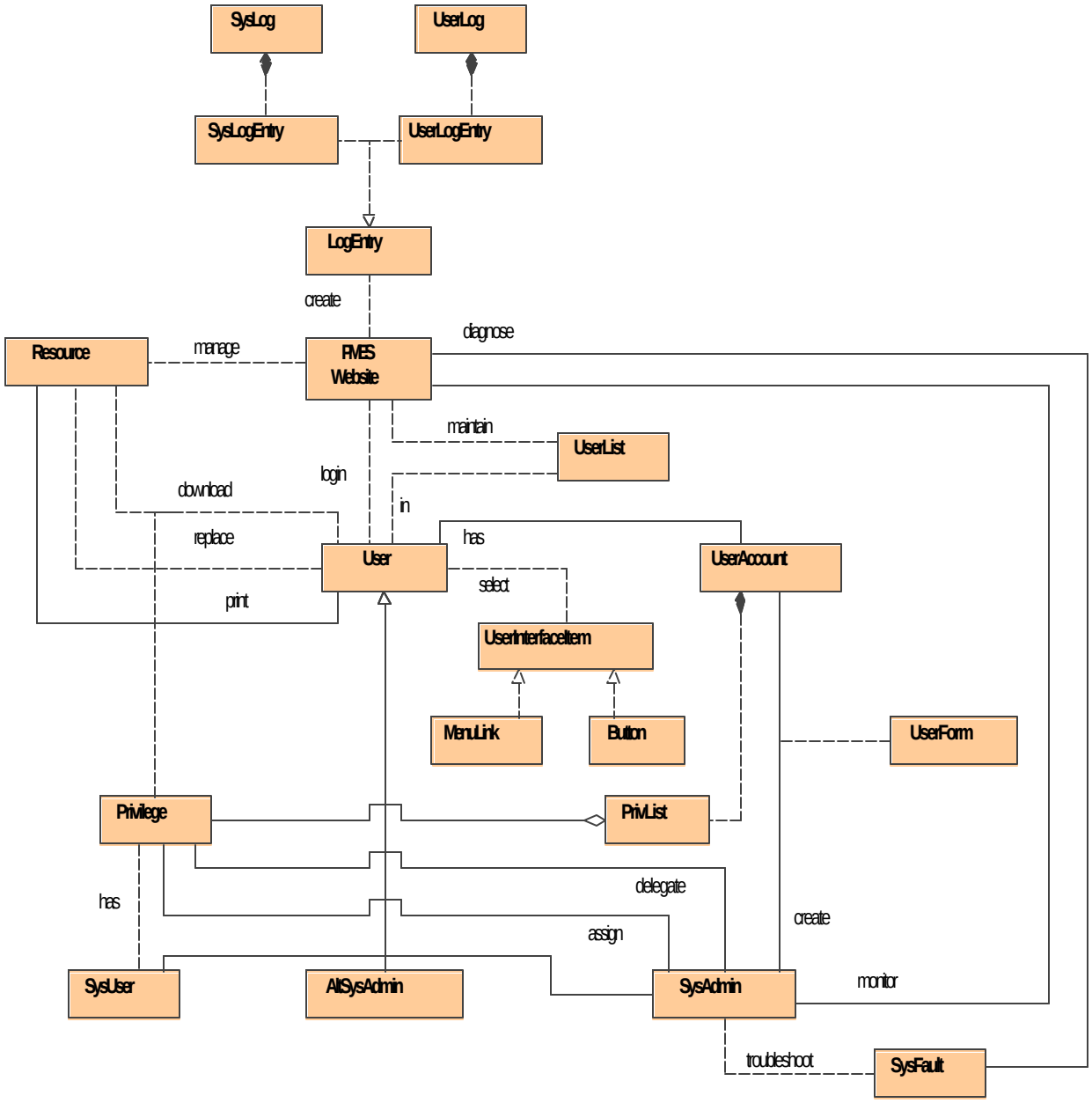


Figure (9)

4. Glossary of Terms, Definitions, Acronyms, and Abbreviations

Authentication: A process whereby the user name and password entered by a user are verified against the appropriate entries in a valid User Account record in the System Database.

DownLoad: The method by which a file is retrieved from the website and stored on the system user's local hard drive.

Authority Delegation: The method by which a System Administrator delegates Privilege Management and Enforcement System authority to another system administrator.

PMES: the Privilege Management and Enforcement System is used to manage and enforce user resource privileges via a web-based user-interface.

Print: The method by which a resource is sent from the PMES to a network printer.

Privilege Level: One of three different security settings (User, Admin, AltAdmin) that can be assign to a User Account by the system administrator.

Privilege List: A list of system resource access privileges that can be assign to a User Account by the system administrator.

Resource: A file, folder, or network device (server, printer, etc.) that can be assigned to and accessed by a system user.

System Log: A log file of all system events recorded by PMES.

Upload: The method by which a file is retrieved from the system user's local hard drive and stored on a PMES file server.

User Log: A log file of all user events recorded by PMES.

Privilege Management and Enforcement System (PMES)

System Design Specification

SW3460

SOFTWARE METHODOLOGY

Prof. Shing

December 27, 2004

(Final)

Jack Chung
Jeff Gorsch
Cop Le

Privilege Management and Enforcement System (PMES) (System Design Document)

TABLE OF CONTENTS

Revision Number	Date	Brief summary of changes

1.0 INTRODUCTION

1.1 PURPOSE

The purpose of this design document is to provide sufficient documentation to produce a working prototype and test it against the system requirements.

1.2 SCOPE OF THE PRODUCT

The scope of the prototype is to model the interface to valid the user privileges and system management of user requirements.

1.3 DEFINITIONS, ACRONYMS, AND ABBREVIATIONS

1.4 REFERENCES

- PMES Project Proposal
- PMES Software Requirements Specifications

1.5 OVERVIEW OF THE SDS

The SDS provides detailed technical data, system information, and other relevant information on PMES. The document includes an architecture diagrams, a design class diagrams, interaction diagrams, state diagrams, and a glossary.

2.0 SYSTEM ARCHITECTURE

PMES is organized into a three-tier closed architecture composed of a presentation layer, domain layer, and storage layer. This organization is intended to provide modularity and manipulation of code should updates be required.

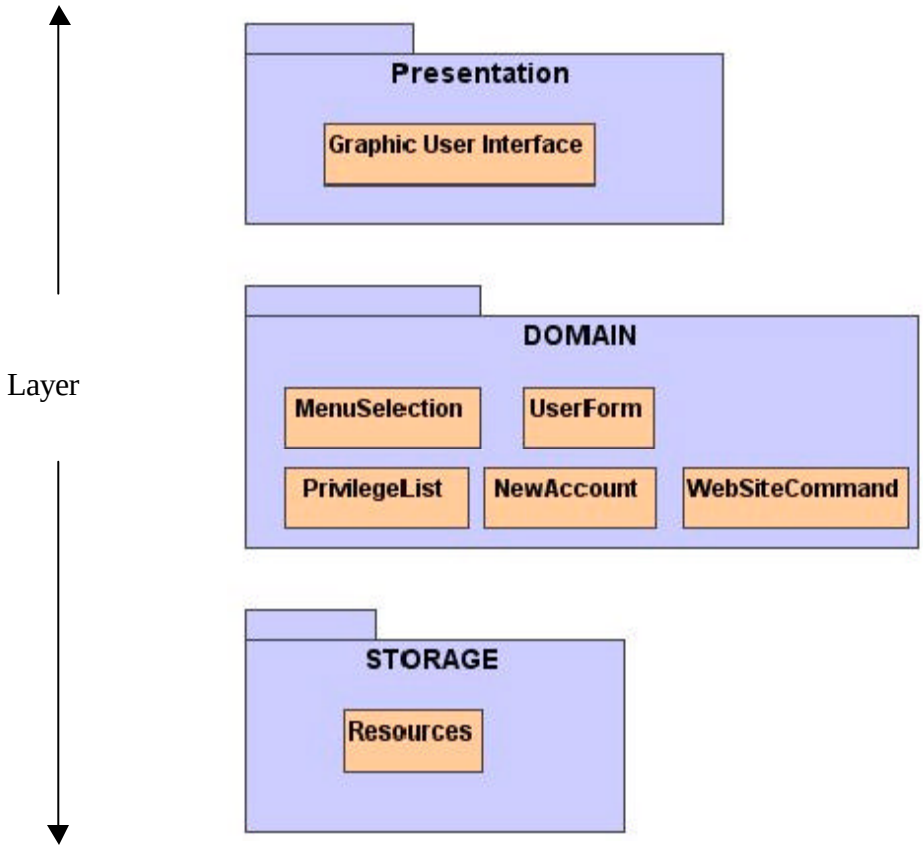


Fig 1. PMES System Architecture

2.1 PRESENTATION LAYER:

The presentation layer includes graphic user interface logic class when action is received.

2.2 DOMAIN LAYER:

The domain layer includes all control and entity objects that conduct privilege list and user form processing, menu selection, rule checking, generate new accounts, website command, and notification require within the domain.

2.3 STORAGE LAYER:

The storage layer includes all stored resource objects that conduct storage, retrieval, and query by the domain objects.

3.0 OBJECT/CLASS DESCRIPTION

Figure 2 shows the PMES conceptual model. It illustrates the basic context of the PMES system operations. The system user enter the website and execute functions and retrieves resources. The system administrator responsible for monitor system user activities, assign user privileges, create new user account, delegate administrator authority to other system administrator if situation is required, and troubleshoot website problems.

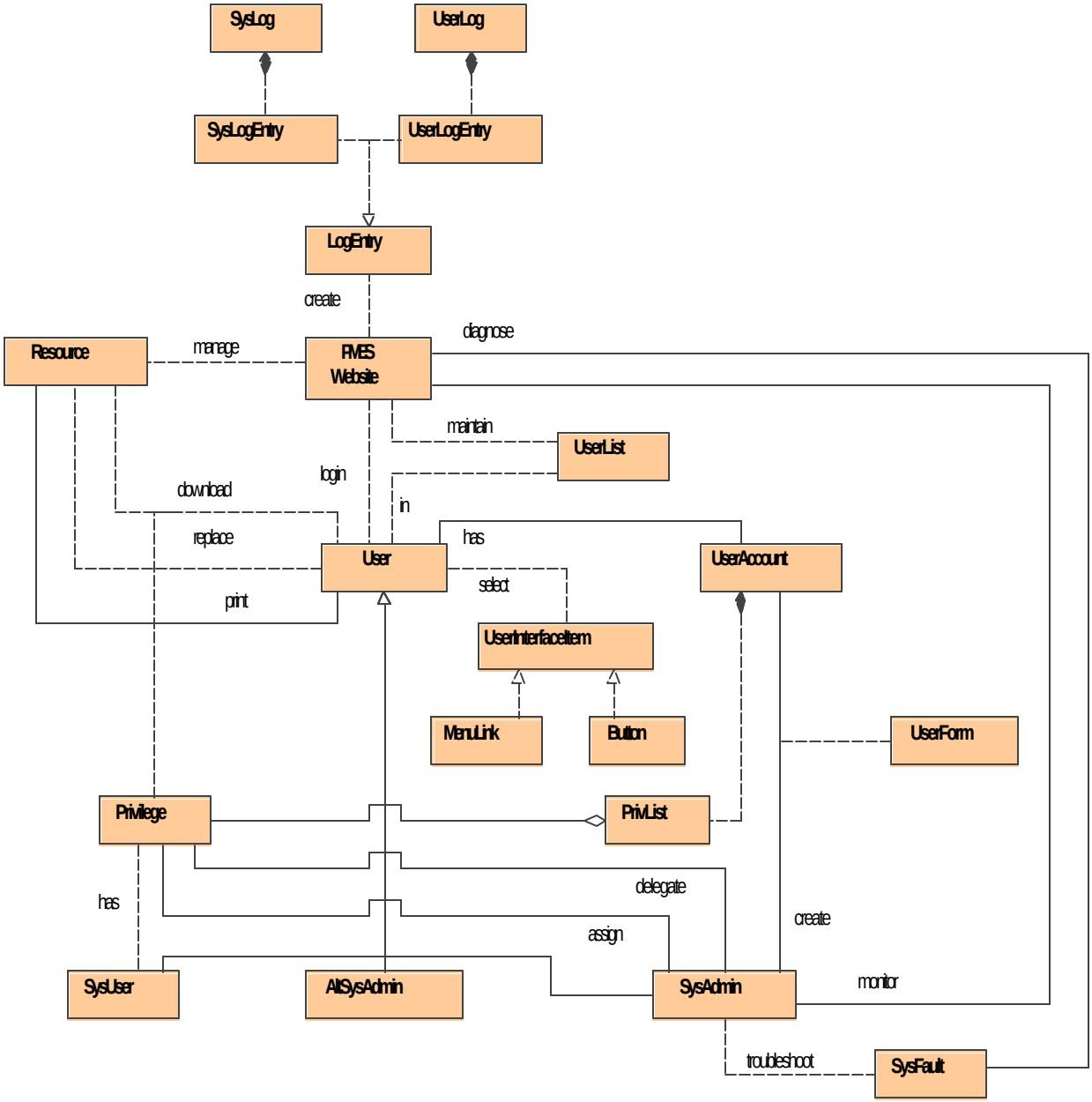


Figure 2 System Conceptual Diagram

3.1 Graphic User Interface

The Graphic User Interface class is located at the presentation layer. Its main function is to provide the System User and System administrator to interface with webpage option selections.

3.1.1 Operation Description

3.1.1.1 processButtonAction()

This method detects a button action and calls the appropriate method of SystemMenu to process the event.

3.1.1.2 changeWebpage()

This method allows webpage to changes to a different webpage that is called by user action.

3.1.1.3 textEntry()

This method allows text or character to be entered by system user on webpage and request prompt.

3.2 User Form

The user form class is located at the domain layer. Its main function is to provide system administration the capability to write text entry on the user form and save to the resource database.

3.2.1 Attribute Description

3.2.1.1 char: letter

The letter attribute is a character that is recorded when user types the letter on the User Form.

3.2.1.2 password: userPassword

user password generated by the system administrator and will be stored in the system.

3.2.1.3 privilegeList:availPrivileges

availPrivileges is a list of privileges available for System Administrator to assign to the System Users.

3.3.1.4 privilege:selectedPrivilege

selectedPrivilege is privilege level selected by System Administrator to be assign to System User and will be stored in the system.

3.2.2 Operation Description

3.2.2.1 enterNewUserForm

This method calls allows System User or System Administrator to enter text or character of username, password, and privilege list.

3.3 Menu Selection

Menu selection class is located at domain layer. Its main function is to provide menu and submenu selection capability to access the resource.

3.3.1 Attribute Description

3.3.1.1 string[]: menuList

menuList is a string array will be display on the menu selection when the user clicks on System Menu.

3.3.1.2 users:userList

userlist is a list of the current user in the PMES and is updates regularly.

3.3.1.3 username:name

name of the current user in the PMES system and will be stored in the system.

3.3.2 Operation Description

3.3.2.1 selectResourceList()

This method calls the menu selection to initiate the process to return a list of resources with name and display it on the website for System User to view.

3.3.2.2 selectCreate()

This method creates a new instance of New User Form and display the form to the user.

3.3.2.3 clickOK()

This method sends action message to PMES and the action message is recorded and processed by PMES.

3.3.2.4 selectUser()

This method calls selected username and record the action.

3.3.2.5 clickPrivilege()

This method calls an action to create current user privilege list and the currently available privilege list.

3.3.2.6 selectPrivilege()

This method calls method of privilege list and allow the system administrator to assign user privilege from the list.

3.3.2.7 monitorUser()

This method calls current user list and their activities from PMES and display it on the website for system administrator to view.

3.3.2.8 selectDelegate()

This method calls delegate authority form and display it on the website for System Administrator to assign delegations to another System Administrator.

3.3.2.9 selectTroubleshoot()

This method calls current system faults and display it on the website for the System Administrator to view and establish link to the help system webpage.

3.3.2.10 selectResourceName()

This method calls the menu selection to initiate the process to return selected resource and its information.

3.3.2.11 selectUserList()

This method calls the menu selection to initiate the process to return a list of current user and display it on the website for System User to view.

3.3.2.12 clickDownLoad()

This method calls the menu selection to initiate the process to download user-selected resource to the user local computer.

3.3.2.13 clickReplace()

This method calls the menu selection to initiate the process to upload user-modified resource from local computer to the website.

3.3.2.14 clickPrint()

This method calls the menu selection to initiate the process to print user-selected resource to a printer.

3.4 Privilege List

Privilege list is located at domain layer. Its main function is to provide privilege information to the system administrator for granting and delegating privileges.

3.4.1 Attribute Description

3.4.1.1 string[]:privilegeLevel

privilegeLevel attribute is a string representation of privilege level provided by the system.

3.4.2 Operation Description

3.4.2.1 createAvailablePrivilege()

This method creates a list of privilege that are available for System Administrator to assign to the System User.

3.4.2.2 getName()

This method get system administrator name from the website command.

3.5 New Account

New account is located at domain layer. Its main function is create and process new user account.

35.1 Operation Description

3.5.1.1 creatNewUserAccount()

This method creates new user account and return confirm message prompt and display on the website for System Administrator to view.

3.6 Website Command

3.6.1 Attribute Description

3.6.1.1 string []: username

username enters by the system user in string characters during user login.

3.6.1.2 string []: password

passwords enter by the system user in string characters during user login.

36.2 Operation Description

3.6.2.1 enterPrompt()

This method enables System User or System Administrator to enter text or character of username and password on the prompt.

3.6.2.2 loginRequest()

This method calls method of login request prompt and return login request for System User to enter username and password.

3.6.2.3 processLogin()

This method take text character enters by system user and calls appropriate method of PMES to process the event.

3.6.2.4 getResourceName()

This method calls the website command to return information from the selected resource name.

3.6.2.5 getResourceList()

This method calls the website command to return a list of resources and display on the website.

3.6.2.6 getUserList()

This method calls the website command to return a list of user with name and display it on the website.

3.6.2.7 getUserName()

This method calls the website command to return information from the selected user name.

3.6.2.8 recordTextEntry()

This method calls the enterNewUserForm method of New User Account by record user keystroke action.

3.6.2.9 getNewUserForm()

This method calls New User Forms and displays it on the webpage for System Administrators to enter System User information.

3.6.2.10 processUserPrivilege()

This method process privilege level users can have and return and display it on the website for System Administrator to view.

3.6.2.11 getUserActivities()

This method calls the website command to return user activities information and display on the website.

3.6.2.12 initiateDownLoad()

This method calls the website command to start the download process for selected resource.

3.6.2.13 initiateUpLoad()

This method calls the website command to start the upload process for selected resource.

3.6.2.14 initiatePrint()

This method calls the website command to start the printing process for selected resource.

3.6.2.15 processDownLoad

This method calls the website command to download the resource to the local hard drive.

3.6.2.16 processUpLoad

This method calls the website command to upload the resource from the local hard drive.

3.6.2.17 processPrint

This method calls the website command to print the resource to a printer.

3.6.2.18 processPrompt

This method calls the website command to process the user prompt action.

3.6.2.19 saveSession

This method calls the website command to save user session during website outage.

4.0 BOUNDARY USE CASE (Website Outage)

Use case: UC-8 Website Outage (boundary)

Primary Actor: System User

Flow of Events:

1. System User lost connection due to website outage.
2. PMES saves System User web page session, which includes last System User action and web page, to temporary database.
3. PMES reconnected to the website and notified the System User.

4. The System User logs into the PMES website (UC-1) and selects "save session…" from the "System" menu.

5. PMES retrieves saved System User web page session from temporary folder.

Entry condition: The System User lost connection to the website due to website outage.

Exit condition: The System User has successfully reconnected and login to the website and view the saved session.

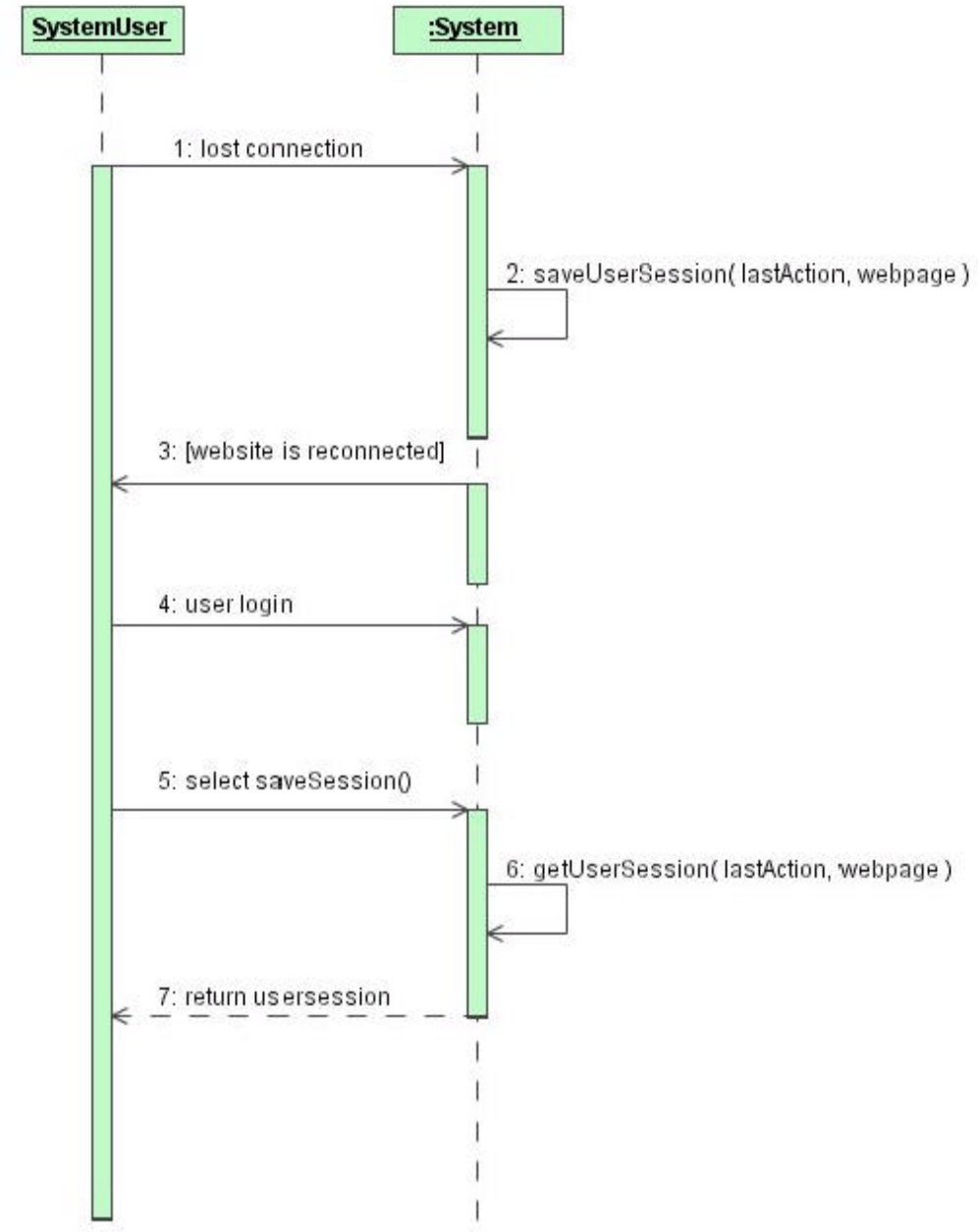


Figure 3a Website Outage Sequence Diagram

Contract: C18 WebsiteOutage
Operation: saveSession()
Cross Reference: UC 8 – Website Outage

Preconditions:
1. Website lost connection.
2. An instance ***w*** of website already exists.

Post -conditions:
1. The saved session was displayed.
2. A new instance ***se*** of session was created.
2. A new instance "save" association ***sv*** was created between ***w*** and ***se***.

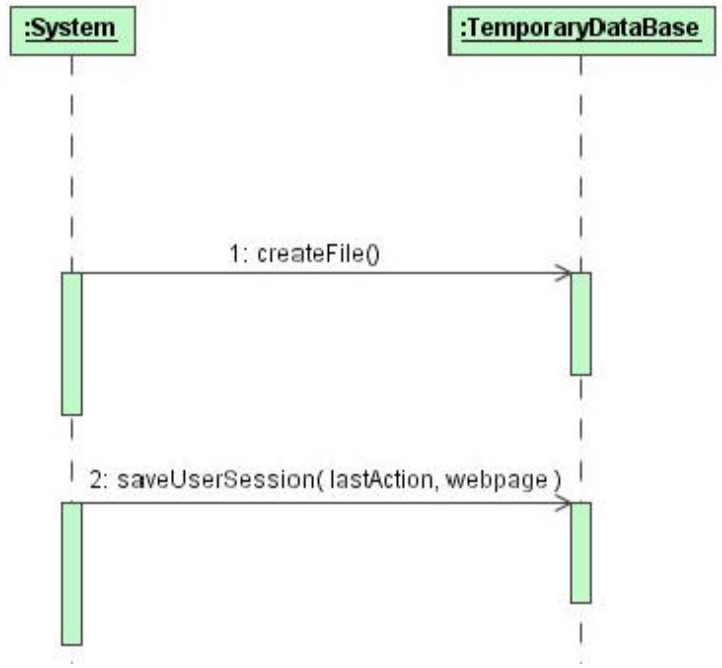


Figure 3b Session Recovery Interaction Diagram

5.0 Requirement Trace Matrix

REQUIREMENTS TRACE MATRIX						
SYSTEM OBJECT CLASS						
SYSTEM OPERATION	**GUI**	**Menu Selection**	**User Form**	**Privilege List**	**NEW ACCOUNT**	**Website command**
selectResources	processButtonAction() changeWebpage()	selectResourceList()				getResourceList()
selectResourceName	processButtonAction() changeWebpage()	selectResourceName()				getResourceName()
selectUsers	processButtonAction() changeWebpage()	selectUserList()				getUserList()
downloadResource	processButtonAction() changeWebpage()	clickDownLoad()				initiateDownLoad() processDownLoad()
uploadResource	processButtonAction() changeWebpage()	clickReplace()				initiateUpload() processUpload()
printResource	processButtonAction() changeWebpage()	clickPrint()				initiatePrint() processPrint()
enterNewUserForm	changeWebPage() textEntry()		enterNewUserForm()			recordTextEntry() getNewUserForm()
selectUser	processButtonAction() changeWebpage()	selectUser()				getUserName()
selectPrivilege	processButtonAction() changeWebpage()	selectPrivilege()		createAvailablePrivilegeList()		processUserPrivilege()
monitorUser	processButtonAction()	monitorUser()				getUserAcitvities()
delegateSysAdmin	processButtonAction()	selectDelegate()		getPrivilegeLevel()		getName()
***selectTroubleshoot	processButtonAction() changeWebpage()	selectTroubleshoot()				
***websiteOutage	processButtonAction()					saveSession()
***loginRequest	processButtonAction()					loginRequest() processPrompt()
***enterPrompt	textEntry()					enterPrompt()
***clickOK	processButtonAction() changeWebpage()	clickOK()				
***createNewAccount	processButtonAction() changeWebpage()	selectCreate()			creatNewUserAccount()	
***clickPrivilegeButton	processButtonAction() changeWebpage()	clickPrivilege()				

***** Will be generated at the next iteration**

6.0 Test Plan

A single set of test procedures will be used for both prototype and system testing. The test procedures were developed directly from the use case descriptions contained in the System Requirements Specification. They are each listed one per page on the following seven pages.

Test 1: User Login	
Preconditions: Internet Access; PMES Web Site Access (Welcome Page)	
Test Step	Action
1.	Click the “Login’ link.
2.	Verify that PMES prompts for User Name and Password.
3.	Enter a valid User Name (for prototype testing, enter “Test”) and Password (for prototype testing, enter “Test”) and click the “Login” button.
4.	Verify that PMES displays the Main Page.

Test 2: Resource Access	
Preconditions: Internet Access; PMES Web Site Access (Main Page), via Test 1	
Test Step	Action
1.	Click the “Resources” link.
2.	Verify that PMES displays a page with a list of available resources (the Resource Page).
3.	Select an available resource by clicking on the resource name and then click the “Download” button.
4.	Verify that PMES downloads the selected resource (does not apply to prototype) and displays a prompt confirming the download.
5.	Click the “OK” button.
6.	Verify that PMES returns to the Resource Page.
7.	Modify the resource on the local computer (does not apply to prototype), click on the previously selected resource name, and then click the “Replace” button.
8.	Verify that PMES uploads the modified resource (does not apply to prototype) and displays a prompt confirming the upload and resource replacement.
9.	Click the “OK” button.
10.	Verify that PMES returns to the Resource Page.
11.	Click on the previously selected resource name and then click the “Print” button.
12.	Verify that PMES sends the resource to the printer (does not apply to prototype) and displays a prompt confirming the action performed.
13.	Click the “OK” button.
14.	Verify that PMES returns to the Resource Page.

Test 3: Create User	
Preconditions: Internet Access; PMES Web Site Access (Main Page), via Test 1	
Test Step	Action
1.	Select the “Users” link.
2.	Verify that PMES displays the Current Users Page.
3.	Click the “Create” button below the Users List.
4.	Verify that PMES displays a “New User” form with entries for User Name and Initial Password, and a list of available privileges.
5.	Enter data for the fields in the “New User” form, select a privilege level, and click the “OK” button.
6.	Verify that PMES displays the **“**New User Created**”** prompt.
7.	Verify that PMES displays the “E-mail notification sent” prompt.
8.	Click the “OK” button.
9.	Verify that PMES returns to the Current Users Page.

Test 4: Assign User Privileges	
Preconditions: Internet Access; PMES Web Site Access (Main Page), via Test 1	
Test Step	Action
1.	Select the “Users” link.
2.	Verify that PMES displays the Current Users Page.
3.	Selects the name of the user for which privileges are to be assigned and click the “Privileges” button.
4.	Verify that PMES displays a list of current privileges for the selected user and a list of privileges available to be assigned.
5.	Select a privilege item from the list and click the “OK” button.
6.	Verify that PMES displays the **“**Confirm privilege assignment**”** prompt to confirm the previous selection.
7.	Click the “OK” button.
8.	Verify that PMES displays the **“**privilege(s) successfully granted**”** prompt.
9.	Verify that PMES displays the “E-mail notification sent” prompt.
10.	Click the “OK” button.
11.	Verify that PMES returns to the Current Users Page.

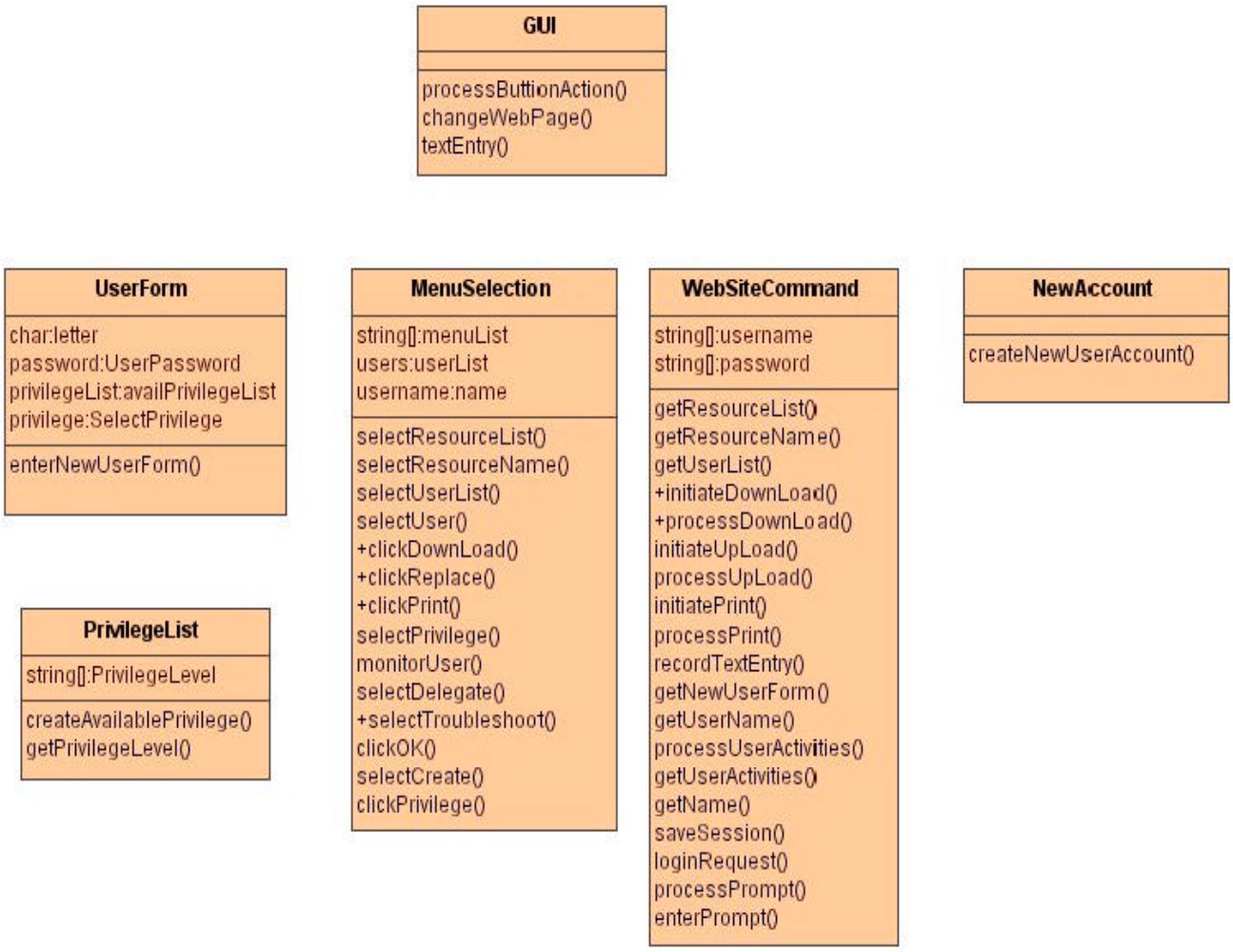
Test 5: Monitor Website	
Preconditions: Internet Access; PMES Web Site Access (Main Page), via Test 1	
Test Step	Action
1.	Select the “Monitor” link.
2.	Verify that PMES displays a monitoring page with a list of current users and their activities.

Test 6: Authority Delegation	
Preconditions: Internet Access; PMES Web Site Access (Main Page), via Test 1	
Test Step	Action
1.	Select the “Delegate” link.
2.	Verify that PMES displays the Delegate Authority Page.
3.	Select assistant / alternate system administrator(s) from the “System Users” list.
4.	Click the “OK” button.
5.	Verify that PMES displays the **“**Confirm delegation of authority**”** prompt to confirm the previous selection.
6.	Click the “OK” button.
7.	Verify that PMES displays the **“**Delegation granted**”** prompt.
8.	Click the “OK” button.
9.	Verify that PMES displays the “E-mail notification(s) sent” prompt.
10.	Click the “OK” button.
11.	Verify that PMES returns to the Main page.

Test 7: Troubleshooting	
Preconditions: Internet Access; PMES Web Site Access (Main Page), via Test 1	
Test Step	Action
1.	Select the “Troubleshoot” link.
2.	Verify that PMES displays a “Troubleshooting” page with a list of current system faults (no faults will be indicated for the prototype).

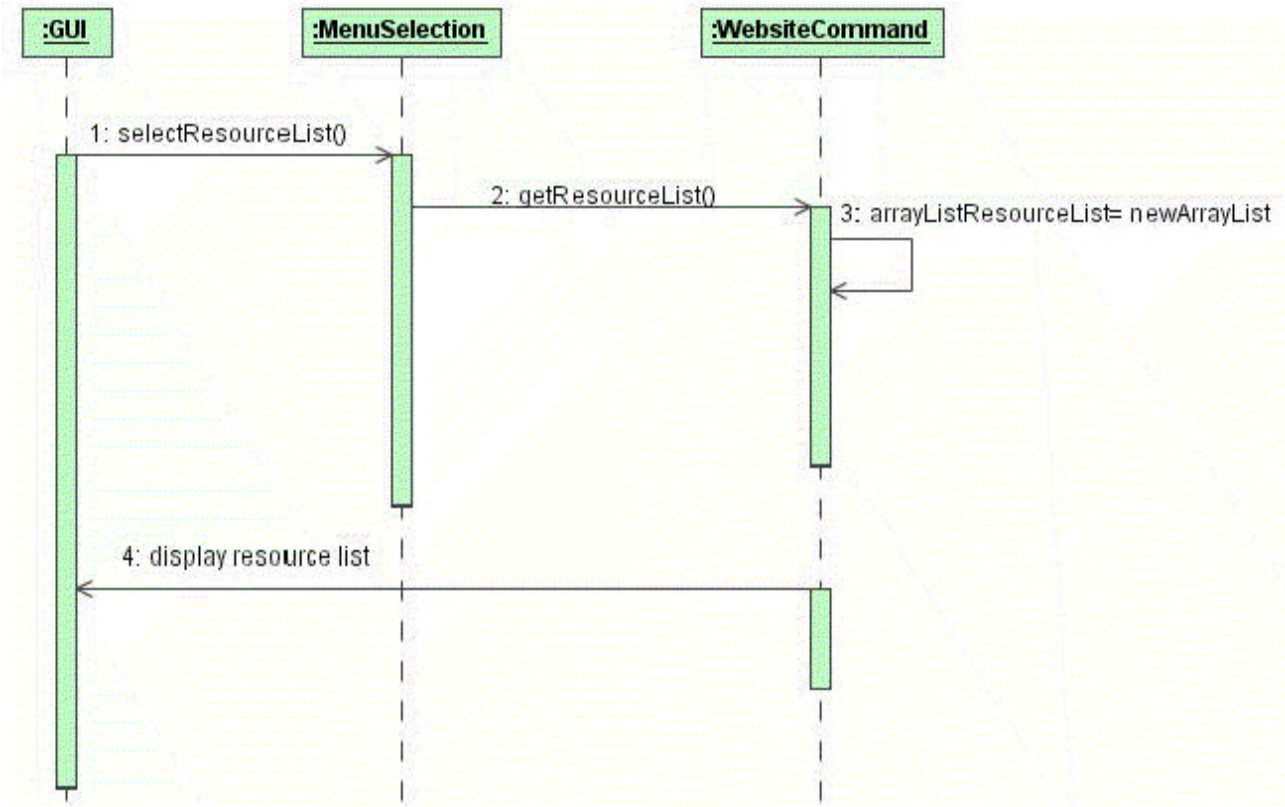
7.0 APPENDIX

7.1 Class Diagram

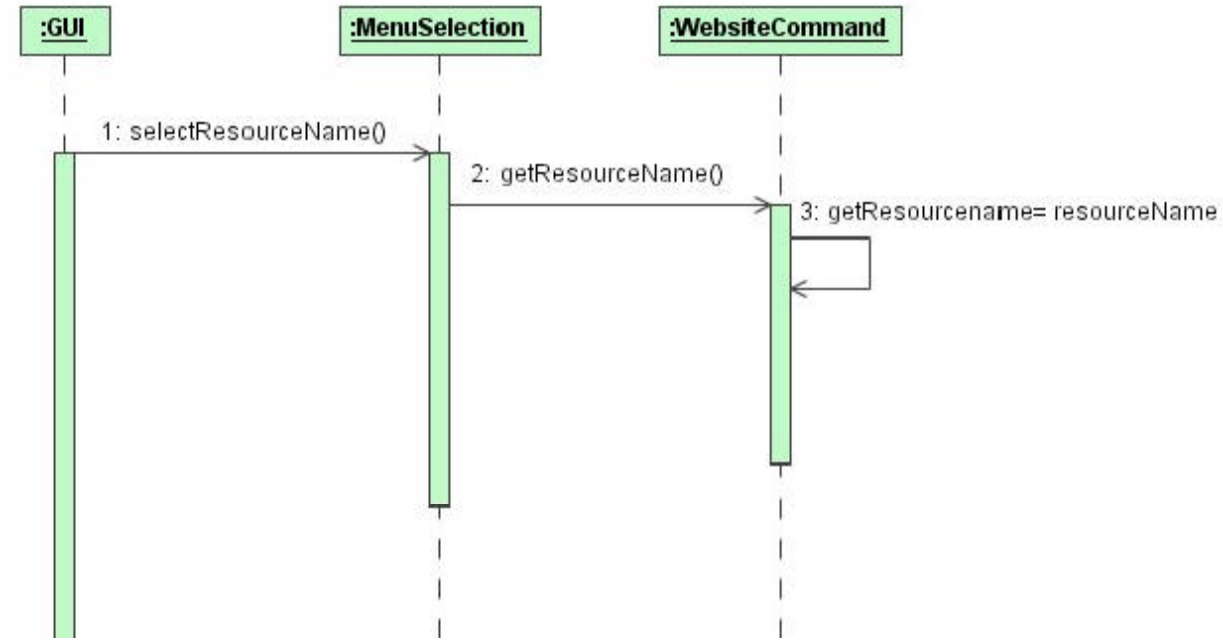


7.2 INTERACTION DIAGRAMS

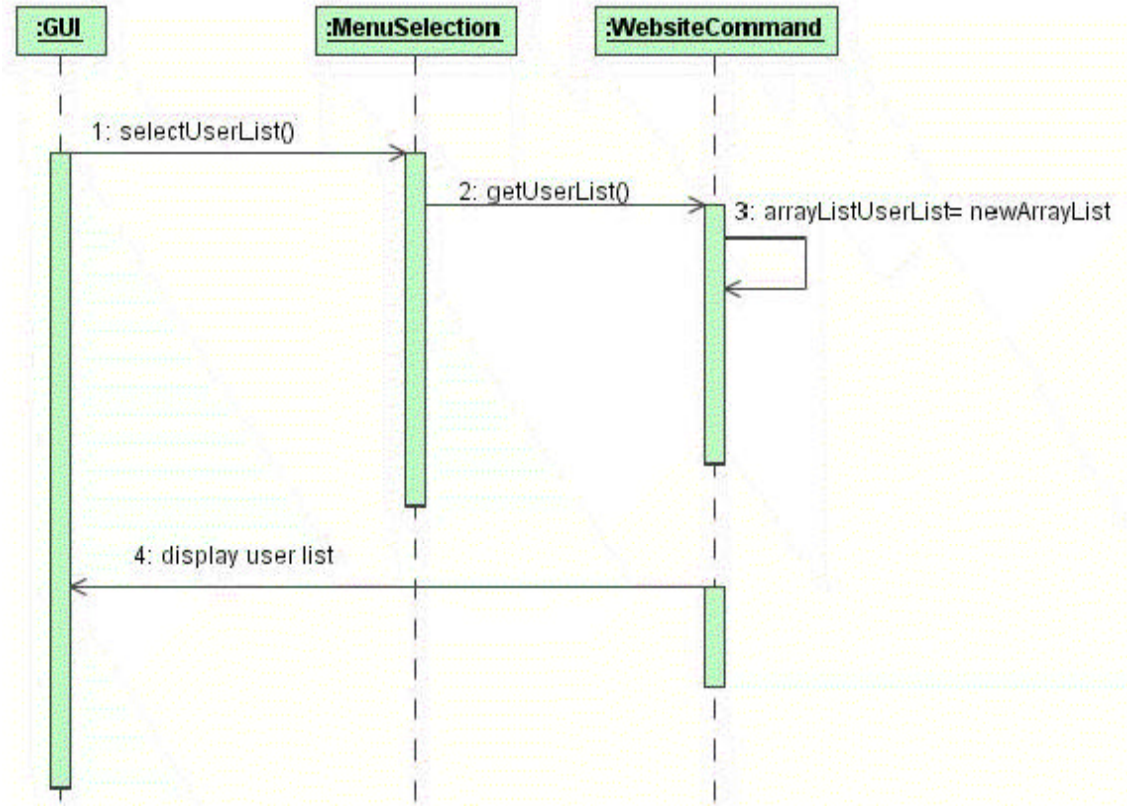
selectResourceList()



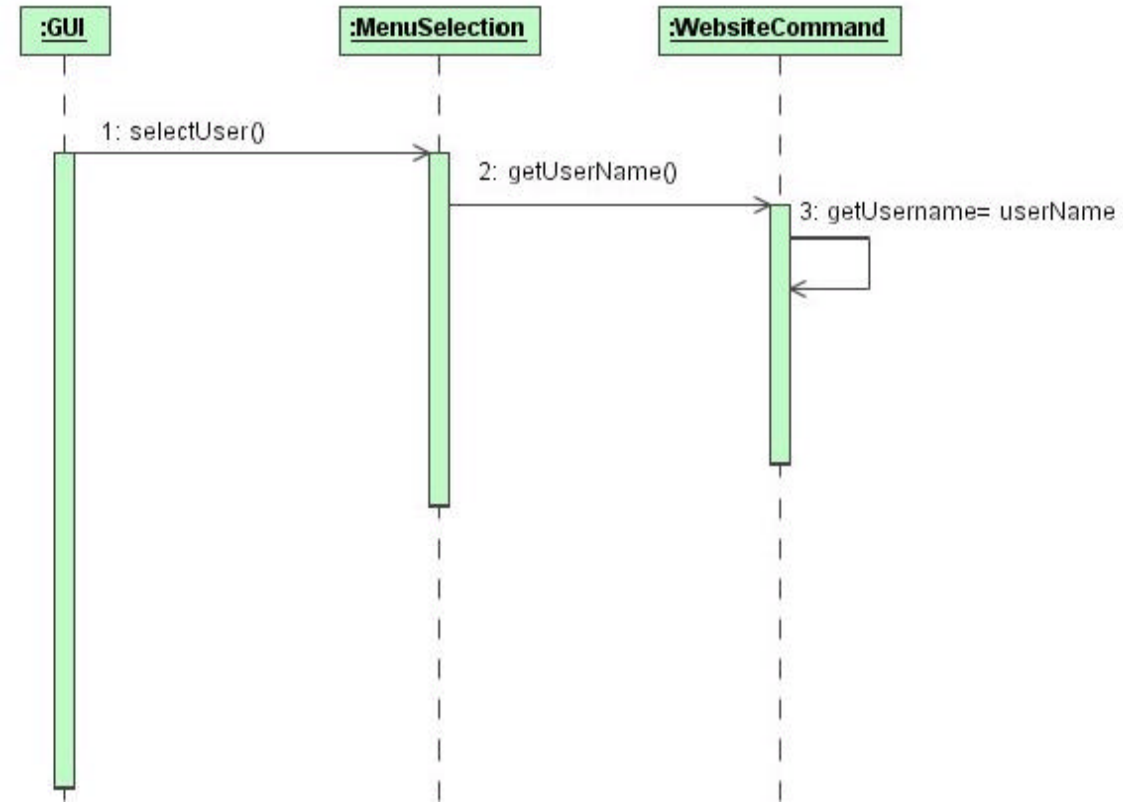
selectResourceName()



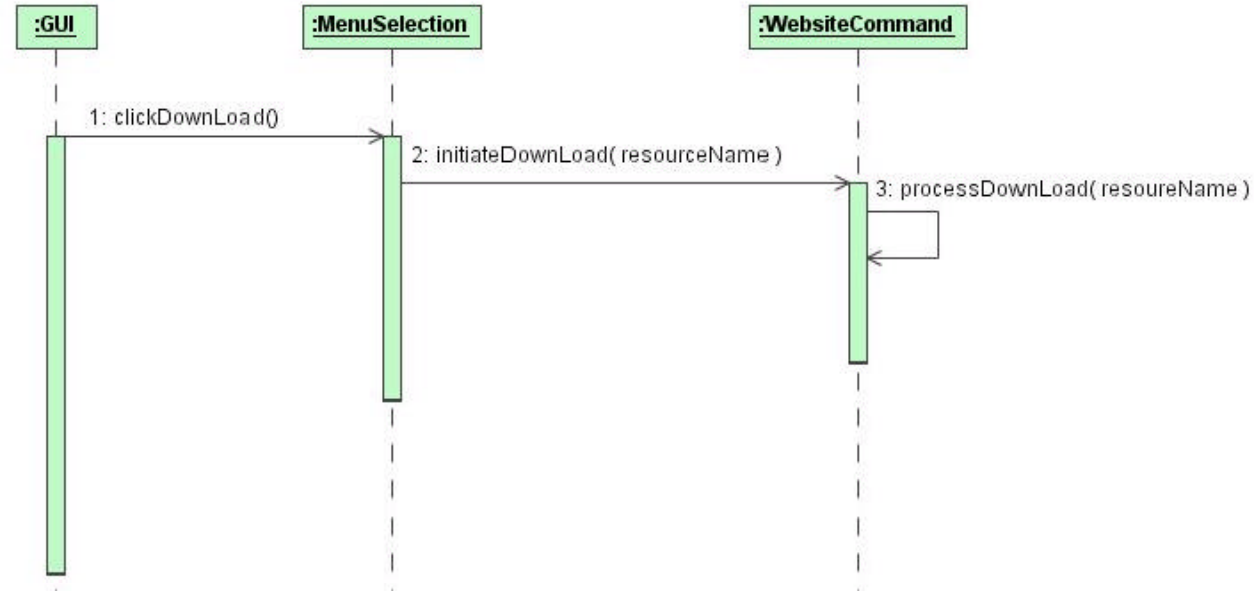
selectUserList()



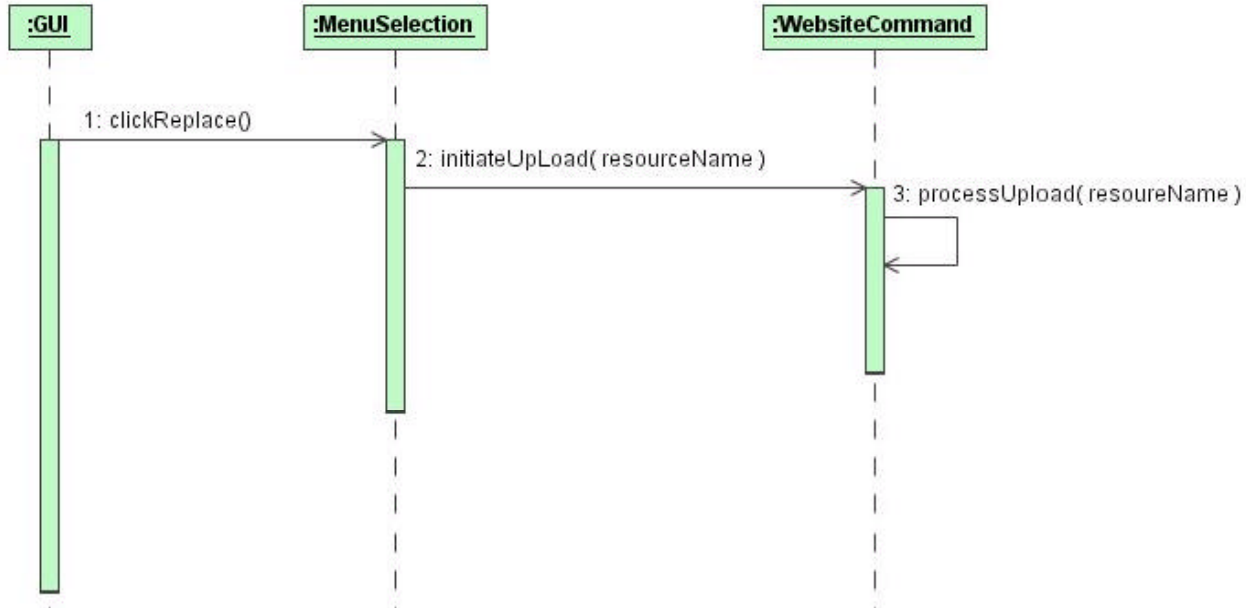
selectUser()



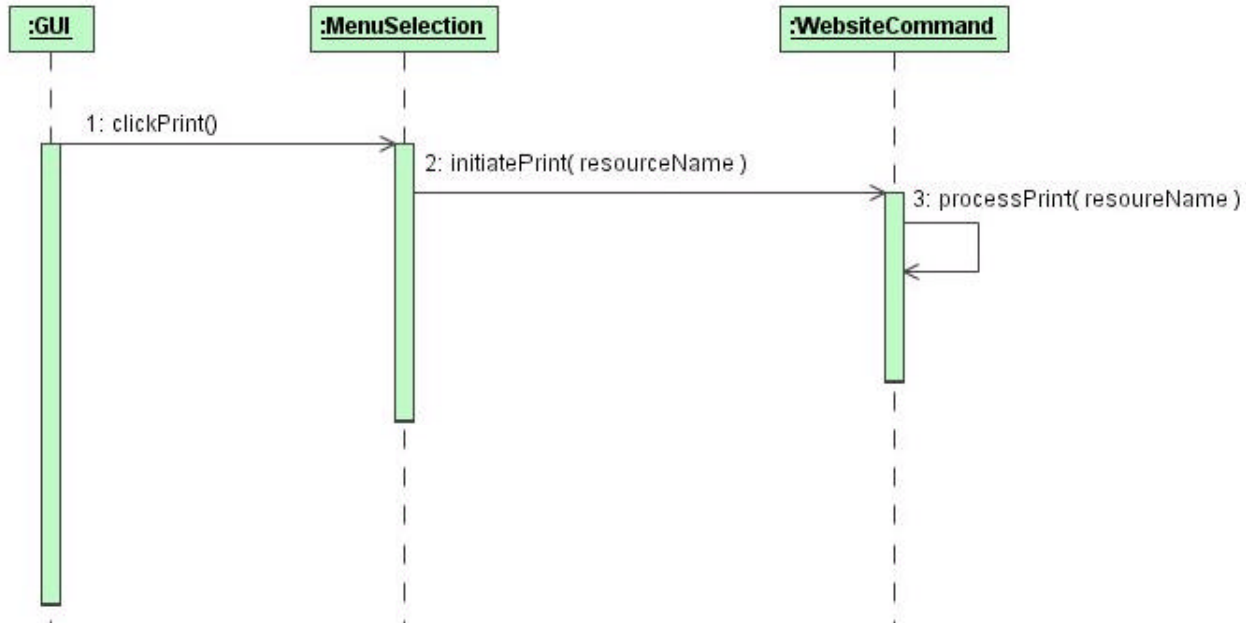
clickDownLoad()



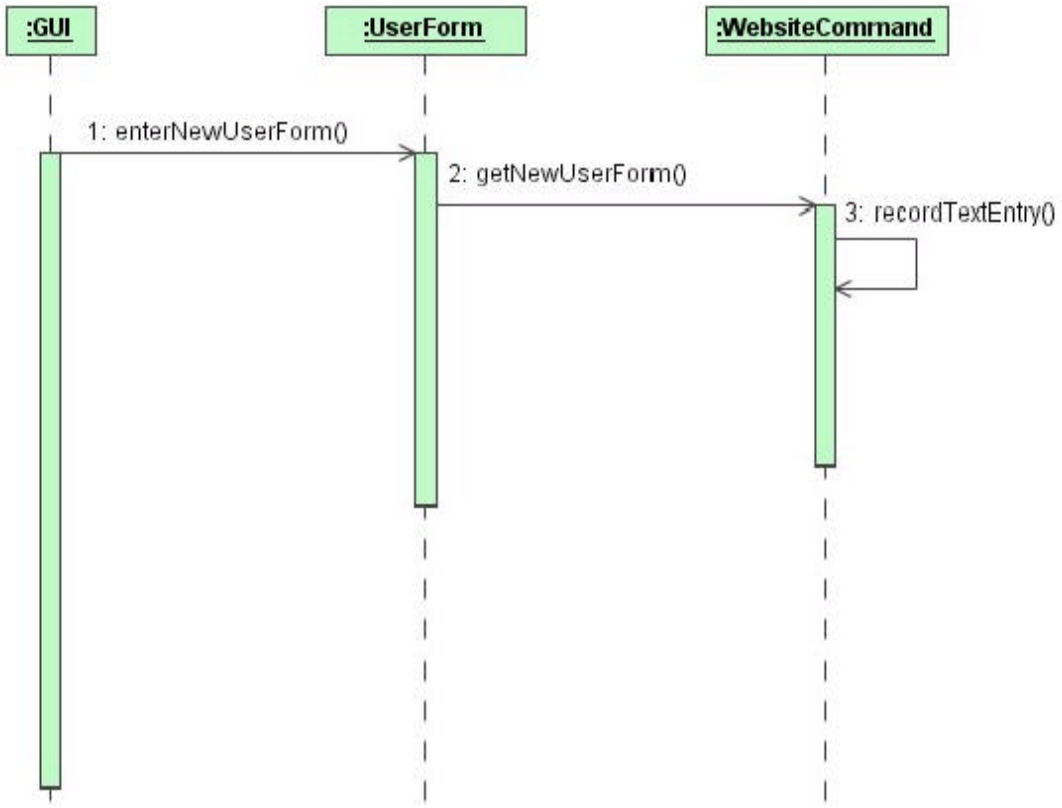
clickReplace()



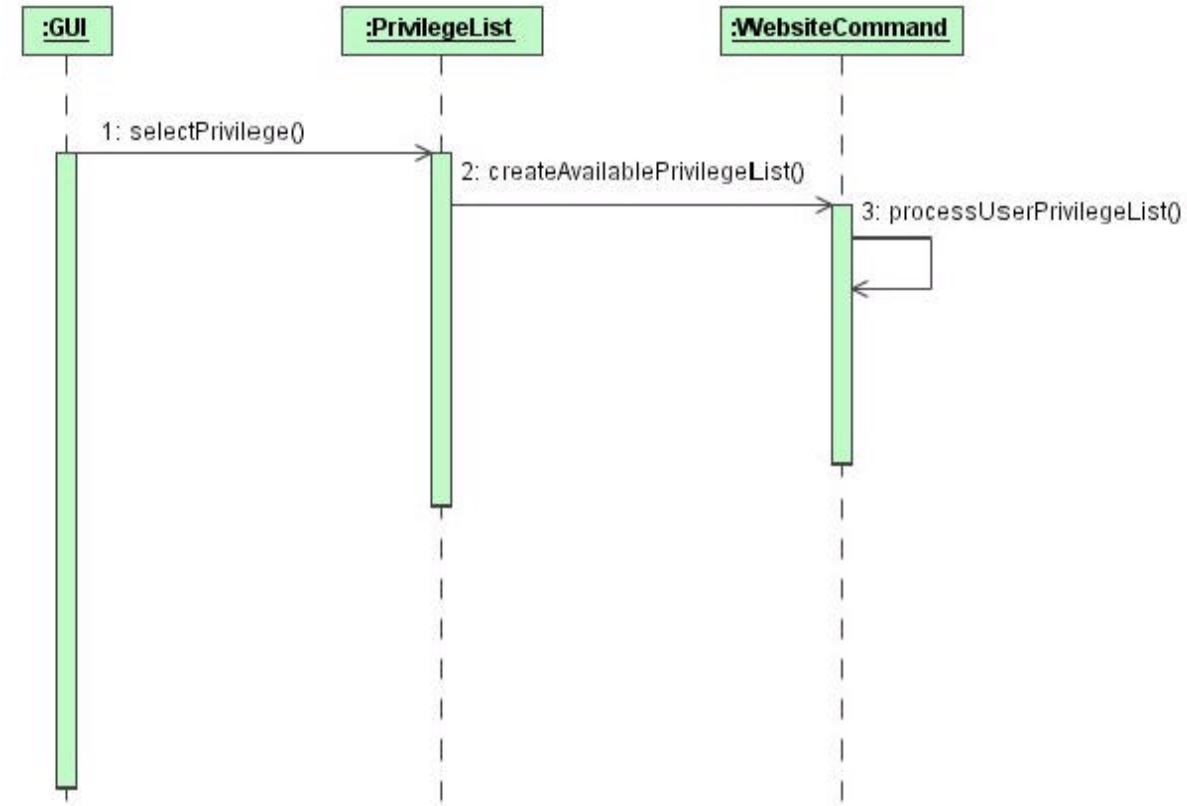
clickPrint()



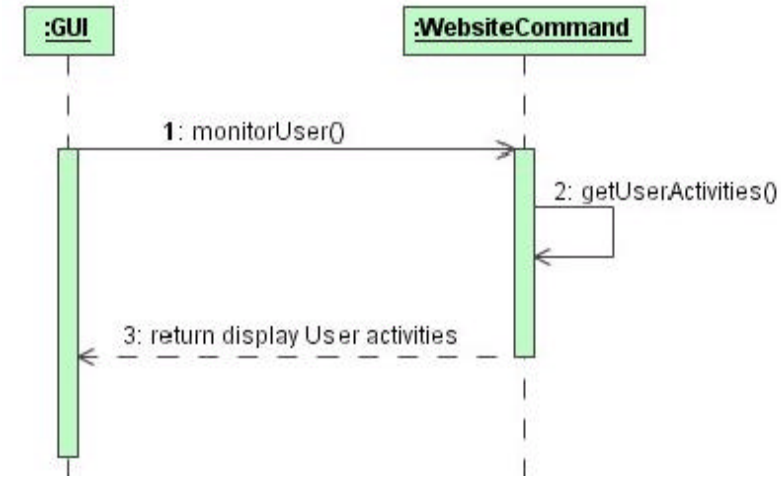
enterNewUserForm



selectPrivilege()



monitorUser()



selectDelegate()