Software Requirements Specification
for
E-Catalog System

CS445/645 Group Project

Team - The Straight A’s

Authors: Yilun Bai

Wenbo Han

Ryan Leung

Kabir Grewal

Table of Contents

1. Introduction

The introduction of the Software Requirements Specification (SRS) provides an overview of the entire SRS with purpose, document conventions, project scopes, definitions, acronyms, abbreviations, references and overview of the SRS. The aim of this document is to gather and analyze and give an in-depth insight of the complete E-Catalog (ECat) by defining the problem statement in detail. Nevertheless, it also concentrates on the capabilities required by stakeholders and their needs while defining high-level product features. The detailed requirements of the E-Catalog (ECat) are provided in this document.

1.1. Purpose

This SRS describes the functional and nonfunctional requirements for software release 1.0 of the E-Catalog (ECat). The purpose of the document is to collect and analyze all assorted ideas that have come up to define the ECat system, its requirements with respect to consumers. Also, this report shall predict and sort out the intended usage of this product in order to gain a better understanding of the project, outline concepts that may be developed later, and document ideas that are being considered, but may be discarded as the product develops.

In short, the purpose of this SRS document is to provide a detailed overview of the software product, its parameters and goals. This document describes the project's target audience and its user interface, hardware and software requirements. This document is intended to be used by the members of the documentation writers who create the initial design of the ECat system, the developers of the programming team who will implement the system, the project managers and the clients who will verify the correct functioning of the system. Unless otherwise noted, all requirements specified here are committed for release 1.0.

1.2. Document conventions

All font shall be in Arial. Title font size shall be in font size 26. Font size 20 shall be used on section names and font size 16 shall be used on subsection names. Normal text shall use font size 12. There shall be an empty line after every paragraph for separation. There shall be a

indentation to separate section and subsection and all the text under the according section should follow the indentation. References shall be in IEEE Access format. Bolded text shall be used when certain words are emphasized. Italicized text shall be used to label and recognize diagrams.

1.3. Project scope

This SRS is created for a web based database system, named E-Catalog, for which the abbreviation of “ECat” shall be used for the rest of the SRS, to catalog physical items that are to filed and stored away [1]. A similar vision and scope document is available and can be referred in *1.4. Reference [1]*.

1.4. References

[1] V. Sakhnini, “Software Requirements Specification and Analysis - Winter 2019, project-document-vision,” *CS 445 / ECE 451 / CS 645*. [Online]. Available: https://www.student.cs.uwaterloo.ca/~cs445/Winter2019/. [Accessed: 03-Apr-2019].

2. Overall Description

2.1. Product perspective

The ECat system is an entirely new software system that is used to catalog the physical items on a web based database system that could be accessed. The ECat will be deployed to a website and all users of the product will access it by use of the website. The website will be the main user interface where users can operate all the provided functionality. However, this website will be only a part of a larger system. There will be cloud server where all the user data is kept and all the execution is done. The website shall be the only interface for the user data and the execution of provided functionalities.

To use product, users are required to register through the web interface. Whenever a new user registered, all the required data will be created in the database. Later, user will be able to login and logout the system anytime he or she wants. The system shall be expected to evolve over several releases, with newly add-in features. Refer to the *Use Case Diagram* and *Domain Model* in *Appendix B: Analysis Models* for further information.

2.2. User Classes and Characteristics

Anonymous User

- New User:
  New Users are those individuals who are part of the general public and do not have an ECat account. They shall have the ability to register an account to become an authorized user.

- Not Logged-in Registered User:
  Not logged-in registered users are those who already have the account, but haven't logged in to the system. They shall have the ability to log-in to their account by correctly entering their username and password, shall have the ability to retrieve and reset their password through the forget password option. They shall also have the ability to receive notifications from the ECat system via emails

delivered to the email address they have registered on their account.

Authorized User (Favored user classes)

- Logged-in Registered User:
  Logged-in Registered users refers to those who correctly entered their username and password and logged in to the ECat system, but not as an admin or super-admin. They shall be able to search and browse objects, manage and navigate to items, send general request to the admin, and log out of ECat system.

- Admin:
  Admin refers to those who have privilege over a logged-in registered user. An admin shall be able to do whatever a logged-in registered user can do. An admin shall be able to manage users, containers, categories, keywords, labels, approve or reject user request, and generate reports.

- Super-Admin:
  Super-Admin refers to those who have privilege over an admin. A super-admin shall be able to do whatever an admin can do. A super-admin shall be able to manage deletion options, manage rules and permissions for different roles, and manage Application Programming Interface (API) keys.

2.3. Operating environment

OE-1: The ECat shall operate on the Microsoft Windows Operating System (NT, 2000, XP or greater).

OE-2: The ECat shall operate on the Macintosh (Mac OS X or greater).

OE-3: The ECat shall operate on all versions of Android, iOS and Windows smartphones and tablets and to that end, shall include mobile page layouts.

OE-4: The ECat shall function correctly with the following web browsers: Windows Internet Explorer version 7, and above; Windows Edge version

version 40, and above; Firefox version 12, and above; Google Chrome (all versions); Apple Safari version 4.0, and above.

OE-5: The ECat shall permit user access from the corporate internet; from a VPN Internet connect.

2.4. Design and implementation constraints

CO-1: The ECat system's design, code, and maintenance documentation shall conform to the IEEE standard.

CO-2: The ECat system shall use a fully relational database back-end.

CO-3: The ECat system shall produce standards-compliant HTML.

CO-4: The ECat system shall provide a development and training environment with the ability to migrate configurations to a production environment.

CO-5: User rights and privileges shall be controlled by Super-Admin.

CO-6: These requirements shall not constrain functionality or features of the Online Public Access Catalog (OPAC) module.

2.5. Assumptions and dependencies

AS-1: When retrieving the password, the user shall know his/her registered email to receive password reset link.

AS-2: Default language for all text displayed on the ECat system shall be in English.

AS-3: The users shall read text from left-to-right, top-to-bottom, unless otherwise stated.

AS-4: The users shall be familiar enough with computers to know how to use a mouse and keyboard.

DE-1: The system shall be running on a modern operating system (Linux or Windows Server) no more than 2 years old, and with active long term support from the operating system vendor.

3. System Features

The functional requirements are grouped by the user role to which they are associated. Please refer to the Sequence Diagram and State Machine Model under *Appendix B: Analysis Models* for further illustration on the control flow of these features in practice.

3.1. Unauthorized User

3.1.1. Description

The unauthorized user is the base role for user profiles and for users who are not yet authenticated, and is mainly used to access login and account creation functionality.

3.1.2. Functional Requirements

- They (the Unauthorized User) shall be able to enter credentials to login with an existing system account
- They shall be able to engage the account creation process, with either a local or supported external account system
- They shall be able to engage the password recovery of system if they have forgotten their password by provided an email address associated with the account.

3.2. Registered User

3.2.1. Description

A Registered User is the least permission role for any authorized profile in the system. This role can interact with the item entities in the system in a basic way (see *Section 3.2.2.* for details), interact with the navigation feature, and send requests to Admin Users.

3.2.2. Functional Requirements

- They (the Registered User) shall be able access the functional requirements stated for the Unauthorized User

- They shall be able to Search for Objects, either by using keyword search or a search over all objects provided they have read permissions on said objects
- They shall be able to Browse Objects for objects and containers they have permissions to read, and view the fields of these objects and containers.
- They shall be able to Manage Items by adding, removing, or editing items and adjust the quantity of each item that is stored.
- They shall be able to request a path from a given location to an object in storage, which will be provided by the Maps API integrated with the system
- They shall be able to send requests to Admin users for the purposes of describing system flaws, recommending new features, or other concerns and questions about the system

3.3. Admin

3.3.1. Description

The Admin is the lowest level of administrator profile roles, and has access which is more advanced than the Registered User but less powerful than the Super-Admin.

3.3.2. Functional Requirements

- They (the Admin) shall have access to all functional requirements specified for the Registered User role
- They shall have the ability to approve or reject user requests, from Unauthorized Users to finalize account creation and from Registered Users for general admin requests
- They shall have the ability to manage users by adding, removing, and modifying profiles, and by editing the role of a given user profile to any role except Super-Admin.
- They shall be able to generate reports of the system for security and auditing purposes, selecting report details from the list of all reportable items

- They shall be able to manage containers to add, remove, and modify their details as well as modifying their contents
- They shall be able to manage keywords and labels by adding, removing, and modifying the details of these keywords and labels as well as the objects to which they are attached
- They shall be able to manage object categories by adding, removing, and modifying the details of categories and to which objects belong in each category

3.4. Super-Admin

3.4.1. Description

The Super-Admin role is the most powerful user profile role in the system and is mainly invoked when first setting up the system parameters and when editing those parameters later on.

3.4.2. Functional Requirements

- They (the Super-Admin) shall have access to all functional requirements specified for the Admin role, and also the ability to promote any user to the role of Super-Admin.
- They shall be able to define system behavior when the containers are deleted from the system, either that deletion is not possible on a non-empty container, or that deletion will remove all child objects with a warning prompt to confirm.
- They shall have the ability to create and modify rules and permissions for different User Roles for the purpose of defining or clarifying the actions which are possible while authenticated as said role
- They shall be able to manage API keys for integration between this system and the external APIs that the system may rely on, including creating, updating, and invalidating keys

3.5. System

3.5.1. Description

The system itself is responsible for sending notifications to users when objects expire, which is not captured by any of the previous groups.

3.5.2. Functional Requirements

- The System shall send notifications to users when prompted by the expiration date of an object, which is an optional field that can be specified for each object. The system notifies each user scoped to that object by the email associated with their account.

4. Data Requirements

4.1. Logical data model

Please refer to *Appendix B: Analysis Models* to view the complete Domain Model for the ECat system.

4.2. Data dictionary

Data Element	Description	Composition or Data Type	Length	Values
Container	Represents a single container in the item inventory.	name decription	name: 256 ASCII characters, or its equivalent in UTF-8	
Item	Represents a single item in the item inventory.	name ID: number description checkedOut: boolean expiryDate	name: 256 ASCII characters, or its equivalent in UTF-8 ID: 64 bits	
Item Expiry Notification	Represents a message sent by the system to users notifying them that an item has expired	message		
Date	Represents a date that may be associated with various entities (see the data model above)			Shall be in the format yyyy:mm:dd
Category	Represents a category with which an item may be associated	name	name: 256 ASCII characters, or its equivalent in	

			UTF-8	
Location	Represents a location associated with an item.	coordinates		The coordinates field must be in the format (x, y, a) where x is the latitude, y is the longitude and a is the altitude.
User Profile	Represents a user profile	username password name email	username: 256 ASCII characters, or its equivalent in UTF-8 password: at least 8 ASCII characters, and up to 16 ASCII characters	
Report	Represents a report generated by the system for an admin or super-admin	reportID: number date title content	reportID: 64 bits	
User Request	Represents a request sent by a user to be approved or rejected by an Admin or Super-Admin	requestID: number requestDepartment requestSubject requestContent	requestID: 64 bits	
API Key	Encapsulates all information relating to a single API key the Super-Admin has created to allow external systems to interact with the system	APIKeyValue: number intendUserOrganization intendedUserSystem intendedUsageDescriptio	APIKeyValue: 256 bits	

		n		
Action	Represents an action that a Super-Admin may set to run when a certain operation is performed by the user (e.g. deletion of a non-empty container)	triggeredOn actionType		
Role	Represents a role that a user profile is associated with. For example, Admins and Registered Users have user profiles associated with different roles, reflecting their differing rights and responsibilities in using the system.	department roleType		
Premissio n	Represents a single right to perform a certain operation associated with a role.	name power	name: 256 ASCII characters, or its equivalent in UTF-8	

4.3. Reports

The system shall be capable of generating various different types of reports for the Admin and Super-Admin to allow them to understand how the system is being used and what users are doing what. Specifically, the system shall be able to generate reports on an individual user including information on that user's permissions and personal details, as well as their usage history of the system. The system shall also be able to generate reports on system usage as a whole, giving statistics on various aspects of system usage over a particular time period or over the entire lifetime of the system. The system shall also generate logs and crash reports that an Admin or Super-Admin may use to troubleshoot any problems that may arise. Finally, the system shall generate reports on various user groups, including information on how many users are in each

group, and their specific usernames, as well as the most and least common operations performed by members of the group, as well as the data entities most often accessed by the group, so that an Admin can evaluate whether the group in question truly needs permission to perform a certain operation or access a certain data entity. The various types of reports the system shall be capable of generating are outlined in the tables below.

Report ID	RPT-1
Report Title	User Activity Report
Priority	Medium
Report Users	Admins and Super-Admins
Data Sources	System internal database
Frequency and Disposition	The report shall be generated on request by an authorized user.
Latency	The report shall be displayed within 5 seconds of request.
Visual Layout	Portrait or landscape mode, depending on the device used to view the report and the orientation of the device.
Header and Footer	The report header shall contain the report ID, report title, the requester's username, and date range specified. The footer shall contain page numbers.
Report Body	Fields shown and column headings: ● Report ID ● Report Date ● Username of the user the report is on ● Total time spent using the system ● Log of operations performed by user ● List of operations run by user (e.g. add, delete, etc), sorted from most to least common ● Last date and time the user was logged on ● Other user information: the user's full name, email, permissions and role
End-of-Report Indicator	None

Interactivity	Ability to truncated or see full logs of user activity and most common commands.
Security Access Restrictions	Only Admins and Super-admins shall be able to generate this type of report. Super-Admins shall be able to generate user activity reports for all types of users, while Admins will be able to do so for all user types except Super-Admins.

Report ID	RPT-2
Report Title	System Usage Report
Priority	Medium
Report Users	Admins and Super-Admins
Data Sources	System internal database
Frequency and Disposition	The report shall be generated on request by an authorized user.
Latency	The report shall be displayed within 5 seconds of request.
Visual Layout	Portrait or landscape mode, depending on the device used to view the report and the orientation of the device.
Header and Footer	The report header shall contain the report ID, report title, the requester's username, and date range specified. The footer shall contain page numbers.
Report Body	Fields shown and column headings: ● Report ID ● Report Date ● Total system uptime during the applicable time period ● Log of operations performed by the system ● List of operations run by the system (e.g. add, delete, etc), sorted from most to least common ● Last login onto the system ● Percentage uptime over the applicable time period and system load (in terms of CPU usage, memory usage)

End-of-Report Indicator	None
Interactivity	Ability to truncated or see full logs of system activity and most common commands
Security Access Restrictions	Only Admins and Super-Admins shall be able to generate this type of report.

Report ID	RPT-3
Report Title	System Troubleshooting Report
Priority	High
Report Users	Super-Admins
Data Sources	System internal database
Frequency and Disposition	The report shall be generated on request by an authorized user
Latency	The report shall be displayed within 5 seconds of request.
Visual Layout	Portrait or landscape mode, depending on the device used to view the report and the orientation of the device
Header and Footer	The report header shall contain the report ID, report title, the requester's username, and date range specified. The footer shall contain page numbers.
Report Body	Fields shown and column headings: ● Report ID ● Report Date ● Total system uptime during the applicable time period ● Log of internal system errors
End-of-Report Indicator	None
Interactivity	Ability to truncated or see the full log
Security Access Restrictions	Only Super-Admins shall be able to generate this type of report.

Report ID	RPT-4
Report Title	User Role Report
Priority	Medium
Report Users	Admins and Super-Admins
Data Sources	System internal database
Frequency and Disposition	The report shall be generated on request by an authorized user
Latency	The report shall be displayed within 5 seconds of request.
Visual Layout	Portrait or landscape mode, depending on the device used to view the report and the orientation of the device
Header and Footer	The report header shall contain the report ID, report title, the requester's username, and date range specified. The footer shall contain page numbers.
Report Body	Fields shown and column headings: ● Report ID ● Report Date ● Name of the user role the report is on ● Number of users in the role ● Total time spent by users in the role, using the system ● Log of operations performed by users in the role ● List of operations run by users in the role, sorted from most to least common ● Last date and time a user in the role was logged on ● The user group permissions
End-of-Report Indicator	None
Interactivity	Ability to truncated or see the full log and operation list
Security Access Restrictions	Only Admins and Super-Admins shall be able to generate this type of report. Super-Admins shall be able to generate user role reports for all user roles, while Admins will be able to do so for all user roles except Super-Admins.

4.4. Data acquisition, integrity, retention and disposal

4.4.1. Data Acquisition

DATA-AC-1: All data in the system shall be acquired by means of user input.

DATA-AC-2: The Super-Admin shall perform initial setup of the system, creating user types, roles, and permissions, and assigning permissions to roles and roles to user types. Thus, the Super-Admin shall be the primary source of user type and role data other data vital to the system's basic functioning.

DATA-AC-3: The Admin user shall perform initial data entry on container information, item categories, and user profiles. Thus, the Admin shall be the primary source of user, container, and category data.

DATA-AC-4: The registered users shall be primarily responsible for data entry on items. While they cannot create, delete, or edit containers, they will be the primary agents responsible for entering data on the items in the catalogue. Day-to-day, they will be the primary users of the system, using it to find items, obtain information on them, find directions for where to obtain them, check items in and out, as well as entering information on new items as they arrive. Thus, registered users shall be the primary source of item data.

4.4.2. Data Integrity

DATA-IT-1: Data integrity shall be ensured by taking backups of all the data in the system. Whether this backup takes place, the number of previous backups to keep, the amount of time for which to keep a backup, how much space to allocate to the backups, and the time interval between backups, shall be configured by the Super-Admin.

4.4.3. Data Retention

DATA-RE-1: Data entered into the system shall be retained according to various policies depending on the type of data in question. Item data shall be retained (backups notwithstanding) until they are deleted by an authorized user. User data shall be retained so long as an Admin or Super-Admin deems fit. A registered user's account shall be retained indefinitely, even if the user stops using the system, until or unless an Admin or Super-Admin deletes it. A user may request an Admin or Super-Admin to remove their profile by sending a request to them.

4.4.4. Data Disposal

DATA-DIS-1: Data entered in the system shall be disposed of simply by deleting it off the system's active storage. Backups that are made that contain the data deleted in the system's active storage may be discarded according to the policy set by the Super-Admin. For example, the Super-Admin may choose to delete a backup after a certain time, or to only keep the last N backups (for some positive integer N), or to move some or all backups to a long-term archiving medium, such as data tapes. The system does not provide any mechanism for selectively deleting data off a certain backup, as that would defeat the purpose of a backup, which is to provide a stable and secure data store from which one may restore data changed in active storage.

5. External Interface Requirements

5.1. User interfaces

UI-1: The system shall provide a uniform look and feel between all the web pages.

UI-2: The system shall provide a digital image for each product in the product catalog.

UI-3: The system shall provide use of icons and toolbars.

UI-4: The user interface for ECat shall be compatible with any browser listed in *2.3. Operating Environment* OE-3 so that the user can make access to the system.

UI-5: The user interface for ECat shall be compatible with the screen with the minimum 800*600 pixels since it is the minimum resolution number that modern monitors are generally compatible with.

UI-6: The ECat system shall provide a navigation bar on each displayed web page to redirect users to the respective page.

UI-7: The navigation bar shall be displayed at the top-left corner of every web page.

UI-8: The ECat system shall provide data validation on registered user information in the login page to make sure that users have authentication to log into accounts.

UI-9: The ECat system shall provide “forgot password” link on the Login Page.

UI-10: The ECat system shall display an error message should validation of the email address fail.

UI-11: The font size shall be at least at 12pt so that users can have a clear view without adjusting the page setting of their browsers.

UI-12: For visibility, all buttons, check boxes, and texts, shall use colors that contrast the background color.

UI-13: The ECat web page shall be able to be scrolled up, down, left and right if the page is not 100% showed on the display.

UI-14: The user shall adjust the setting in the web browser to zoom in or out the web page.

UI-15: A search bar that could display at least 50 characters shall be placed at the middle-top of the web page.

UI-16: There shall be a logout option on the top right corner on every web page after logged in.

UI-17: A list of search result pertaining to the query shall be displayed when the user enters a search query.

UI-18: The user interface design for regular user, admin and super-admin shall be consistent, with minor changes (See UI-19).

UI-19: The extra management features for the admin and super-admin shall be concatenated into a “manage” drop-down menu. By selecting the management feature, the ECat system shall take the user to the page accordingly.

UI-20: No text shall overlap with each causing illegibility.

UI-21:The ECat system name “E-Catalog” and logo shall be displayed on the top-left corner of every page.

UI-22: When linking to another webpage is requested, the webpage shall be a pop-up screen and to be displayed on top of our ECat screen.

5.2. Software interfaces

SI-1: The ECat system shall retrieve the current device Global Positioning System (GPS) location, and send it through the API connection to the external Map system.

SI-2: The ECat system shall be able to retrieve the user name and email account from the external information system as login information.

5.3. Hardware interfaces

HI-1: The device that is used to access the ECat system shall be connected to the internet.

HI-2: The server the system is running on shall be connected to the internet.

5.4. Communications interfaces

Reference the *Sequential Diagram* in *Appendix B: Analysis Models* for details.

CI-1: The ECat shall send an email to user's registered email account for account registration.

CI-2: The ECat shall send an email to user's registered email account for password recovery.

CI-3: The ECat shall send an email to user's registered email account for item notifications (based on user setting).

CI-4: The ECat shall send an email to user's registered email account for request processed notification.

CI-5: All emails shall be sent in a consistent format, listing with the date, the sender, the recipient and the matters.

CI-6: Attachments in the email shall not be permitted.

CI-7: The ECat system shall use the HTTP protocol for communication over the internet and for the internet communication will be through TCP/IP protocol suite.

CI-8: The ECat shall generate an Add Item Detail page for registered users to add items to system.

CI-9: The ECat shall generate a Modify Item Detail page for registered users to modify items to system.

CI-10: The ECat shall generate a Delete Item Detail page for registered users to delete items to system

CI-11: The ECat shall generate a Decline Reason Form for admin to reject requests from users.

CI-12: The ECat shall generate an Add User Detail page for admin to add users to system.

CI-13: The ECat shall generate a Modify User Detail page for admin to modify users' information.

CI-14: The ECat shall generate a Delete User Detail page for admin to delete users.

CI-15: The ECat shall generate an Add Container Detail page for admin to add containers to system.

CI-16: The ECat shall generate a Modify Container Detail page for admin to modify containers' information to system.

CI-17: The ECat shall generate a Delete Container Detail page for admin to delete containers.

CI-18: The ECat shall generate an Add Keyword/Label Detail page for admin to add keyword or label to system.

CI-19: The ECat shall generate a Modify Keyword/Label Detail page for admin to modify keyword or label to system.

CI-20: The ECat shall generate a Delete Keyword/Label Detail page for admin to delete keyword or label.

CI-21: The ECat shall generate an Add Category Detail page for admin to add categories to system.

CI-22: The ECat shall generate a Modify Category Detail page for admin to modify categories to system.

CI-23: The ECat shall generate a Delete Category Detail page for admin to delete categories to system.

CI-24: The ECat shall generate a Rules and Permissions Detail page for super-admin to add or modify rules and permissions to system.

6. Quality Attributes

6.1. Usability

USE-1. At least 85% of new users shall judge the system to be usable.

USE-2. At least 80% of new users shall be able to perform data entry (adding, removing and editing items) using the system after one week of training.

USE-3: At least 75% of new Admins with at least 2 years of experience in the field shall be able to correctly add, edit and delete user profiles and containers as appropriate, after 2 weeks of training.

USE-4: At least 75% of new Super-Admins with at least 3 years of experience in the field shall be able to correctly set up the system as appropriate for the user(s) or organization(s) in question, after 3 weeks of training.

6.2. Performance

PER-1. The system shall by default be configured such that all the requirements below are met with a planned peak load of 2000 logged on simultaneous users.

PER-2. The system shall respond to any user action (that is, to give some acknowledgement that it has received the user's input and begin but not necessarily finish performing the appropriate processing) in 16 milliseconds.

PER-3. The system shall return all search results for an item, container, or keyword within 0.5 seconds on average.

PER-4. The system shall finish performing operations to items, containers, and other data items (add, delete, edit) in an average of at most 0.2 seconds.

PER-5. The system shall have a minimum throughput of 500 operations per second under planned peak conditions.

6.3. Security

SEC-1. The system shall request and verify the identity of users attempting to access the system using a username and password, two-factor authentication, or another trusted external system (such as a Google account).

SEC-2. The system shall verify the permissions of the user to perform any requested action (e.g. adding or removing an item, creating a new container, etc) before performing it.

SEC-3. The system shall forcibly log out a user and require the user to verify their identity (for example, via a validation link sent to their email address) before allowing them to log in again, if it detects unusual activity from their user profile.

6.4. Availability

AVL-1. The system shall be available at least 99% of the time when there is active support staff working to keep it online (e.g. during weekdays, and possibly other days in a large organization)

AVL-2. The system shall be available at least 95% of the time even when there is no active support staff (e.g. on weekends or other holidays in small organizations), and shall include redundant servers which shall automatically restart when a fatal problem is encountered and periodically to ensure that this remains the case.

AVL-3. The system shall continue to meet the above availability requirements even in conditions of continuous operation at the planned peak load.

6.5. Safety

SAF-1. The system shall not present any flashing images or other visual patterns that may be harmful to people with epilepsy or other neurological disorders.

6.6. Scalability

SCA-1. The system shall be able to accomodate a growth rate in peak simultaneous users of 20% per year for at least 2 years without visible performance degradation.

SCA-2. A new redundant server shall be able to be added to the system or replaced by a trained IT professional in at most 12 hours.

SCA-3. The system shall be able to accomodate a 100% growth in number of data entities in the system (e.g. containers, items, users, etc) per year for at least 2 years without visible performance degradation.

6.7. Others

OTH-1. Long-term support, in the form of software updates and technical support shall continue to be provided for at least 6 years after the release of the system.

OTH-2. No more than two years shall elapse between major system releases.

7. Internationalization and Localization Requirements

This system should be outfitted with a number of different measures to ensure compatibility with international client locations.

1. Localization options shall be provided to the user under a settings page. The user shall be able to set their country of residence, which will determine the options chosen in the following requirements. The user shall be able to change these other requirements manually as well. For example, a Spanish speaker in Canada shall be able to set their language accordingly.

2. Chinese (Mandarin), Spanish, English, Hindi, Arabic, Portuguese, Japanese, French, German, and Russian text translations shall be included by default. For languages that do not use the English alphabet, character conversion shall be included as well.

3. Date and Time localizations shall also be added in addition to these language packs, which would include Month/Day/Year order in dates, Timezone specifications, whether or not to apply Daylight Saving time, etc.

4. The Maps API and Route to Item functionality shall support distances in Metric and Imperial units.

5. Telephone numbers, if they appear on a user’s profile, shall be formatted according to the standard of the country to which they belong.

6. For countries which list the family name before the given name, user profile name fields shall be displayed accordingly.

8. Other Requirements

8.1. Diagrams and Models

Due to the size of the Use-case Diagram, the Sequence Diagram, the Domain Model, and the State-machine Model are not the same with SRS, they will be appended to this SRS in *Appendix B: Analysis Models* as attachments. These for files will be in the order as they are listed. Viewers can use Adobe Acrobat Reader DC to view this SRS and zoom in to have a clear view on those diagrams and models.

8.2. Legal Disclaimer

LD-1: The ECat system shall not regulate items that is being filed onto the system, meaning that the ECat system shall not know any of the legal issues of the items.

LD-2: If user uses the ECat system to file any illegal items, our system shall not perform any differently.

LD-3: ECat does not accept any responsibility or liability for the content, safety, reliability, and legality of the items being filed on the system.

LD-4: ECat shall not be liable for any loss or damage of whatever nature (direct, indirect, consequential, or other) whether arising in contract, tort or otherwise, which may arise as a result of your use of (or inability to use) this website, or from your use of (or failure to use) the information on this site.

LD-5: The ECat website provides API connection with external websites or systems owned by third parties. The content of such third party sites is not within our control, and we cannot and will not take responsibility for the information or content thereon.

LD-6: The ECat system will not guarantee that this website is free from computer viruses or anything else that has destructive properties.

8.3. Privacy Policy

PP-1: The ECat shall use web cookies to identify user and track visitors' behaviors, and shall notify the user when they register account.

PP-2: The ECat shall collect personal information while using external system, and it shall get approval from users.

PP-3: The ECat shall promise that the collected information will not be unveiled to any third party.

PP-4: The ECat shall inform users the information it collected.

PP-5: The ECat system shall directly collect analytics data, or use third-party analytics tools, to help it measure traffic and usage trends for the service.

PP-6: The tools shall collect information set by the user's browser or mobile devices, including the pages you visit and other information that assists it in improving the service.

PP-7: The ECat shall collect and use the analytics information in aggregation form such that it cannot reasonably be manipulated to identify any particular individual user.

Appendix A: Glossary

1. Abbreviations & Acronyms

a. SRS - Software Requirements Specification
b. ECat - E-Catalog
c. OE - Operating Environment
d. CO - Design and implementation constrains
e. AS - Assumptions
f. DE - Dependencies
g. DATA-AC - Data Acquisition
h. DATA-IT - Data Integrity
i. DATA-RE - Data Retention
j. DATA-DIS - Data Disposal
k. UI - User interface
l. SI - Software interface
m. HI - Hardware interface
n. CI - Communication interface
o. USE - Usability
p. PER - Performance
q. SEC - Security
r. AVL - Availability
s. SAF - Safety
t. SCA - Scalability
u. OTH - Others
v. LD - Legal Disclaimer
w. PP - Privacy Policy
x. GPS - Global Positioning System
y. API - Application programming interface

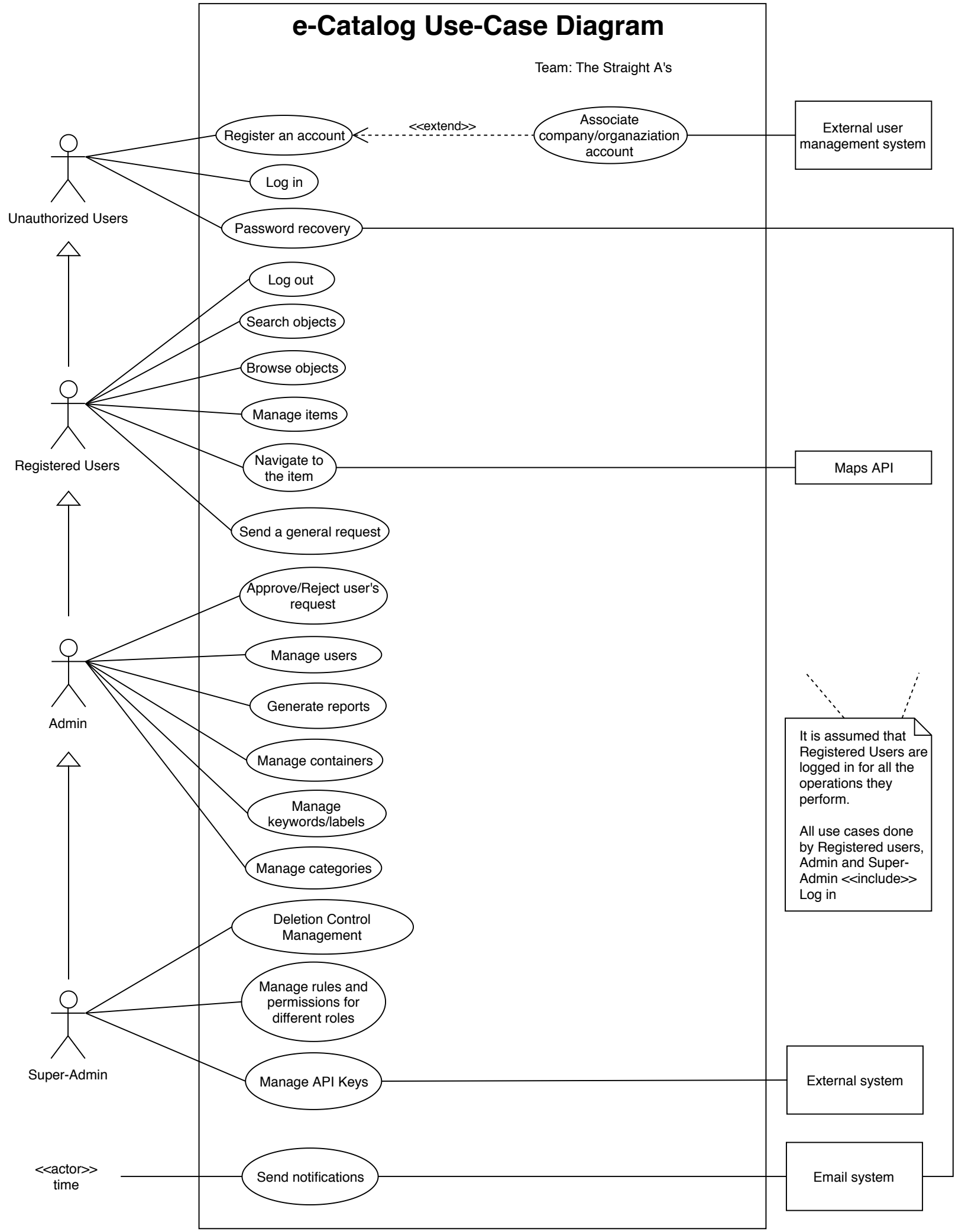
Appendix B: Analysis models

See *Section 8.1. Diagrams and Models* for explanation.

1. Use-Case Diagram
2. Sequence Diagram
3. Domain Model
4. State-Machine Model

e-Catalog Use-Case Diagram

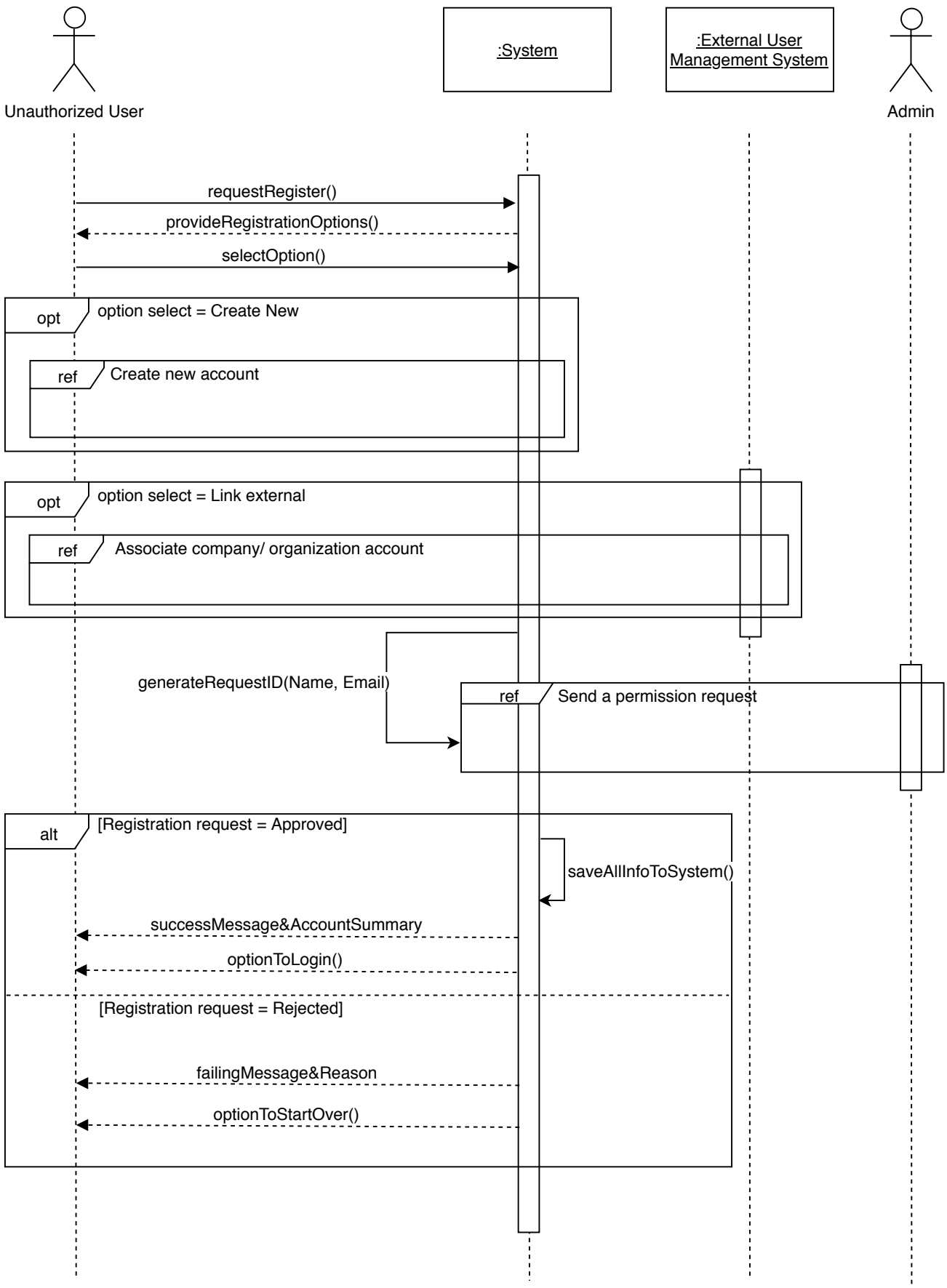
Team: The Straight A's

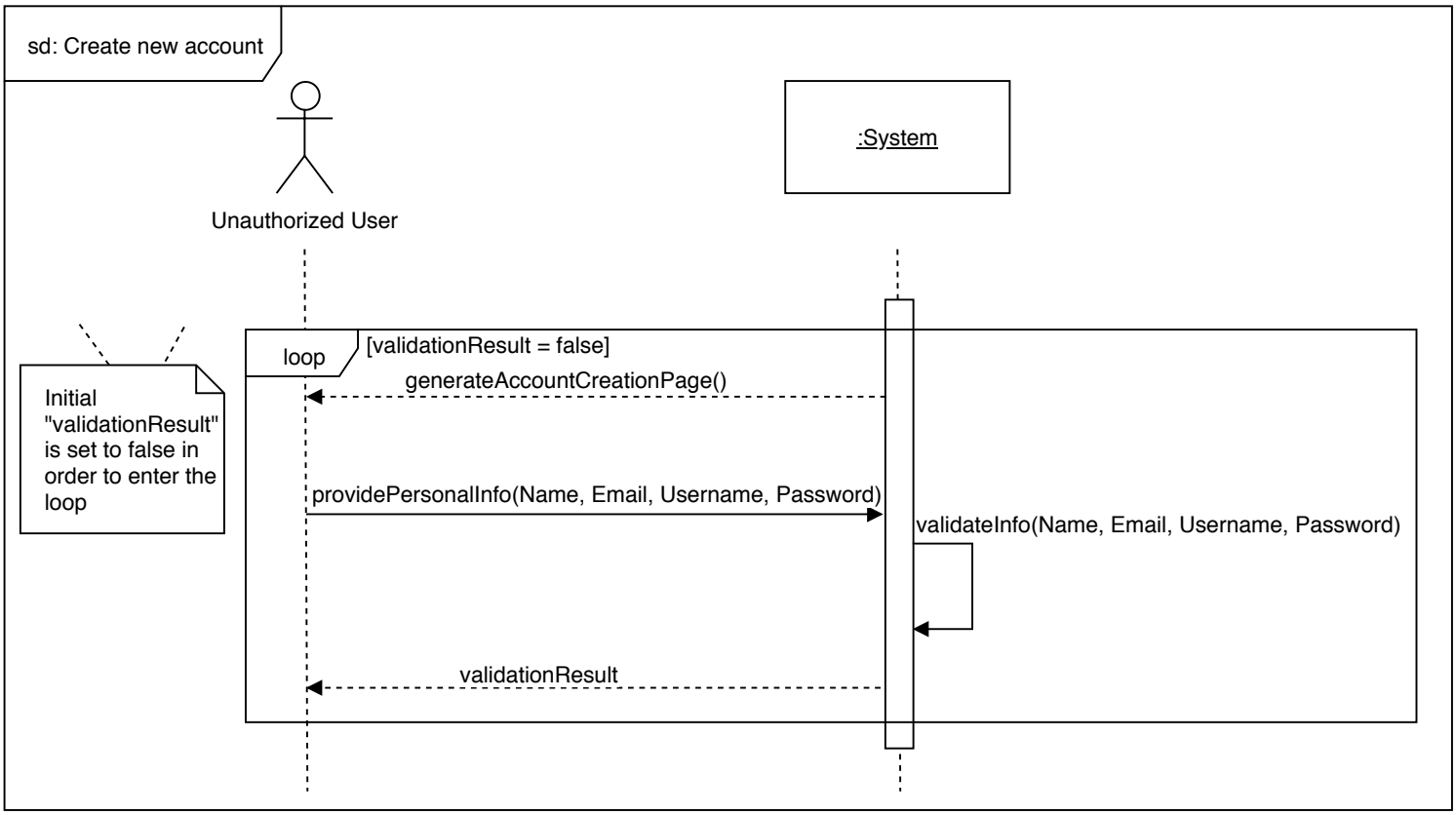


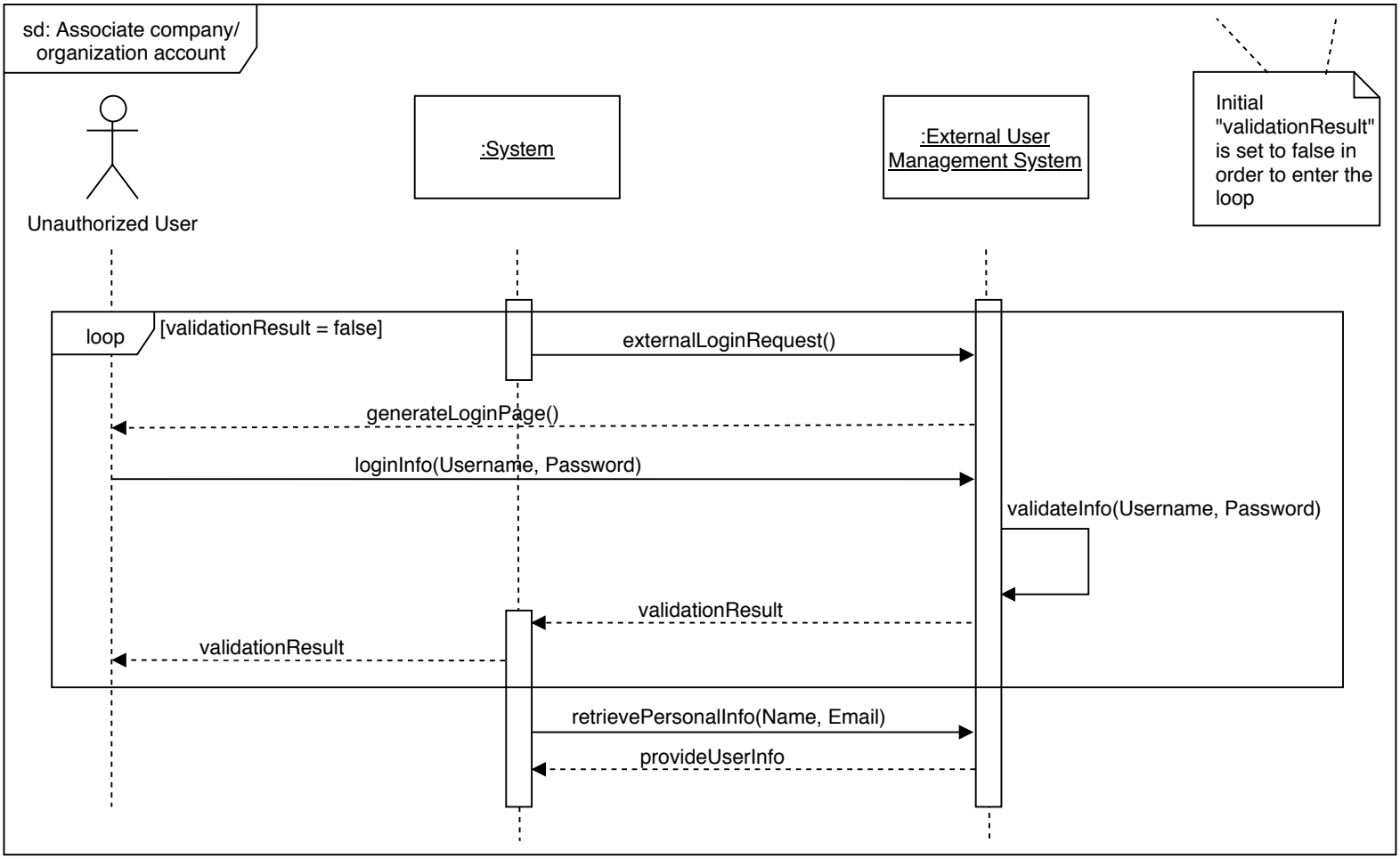
e-Catalog Sequence Diagram

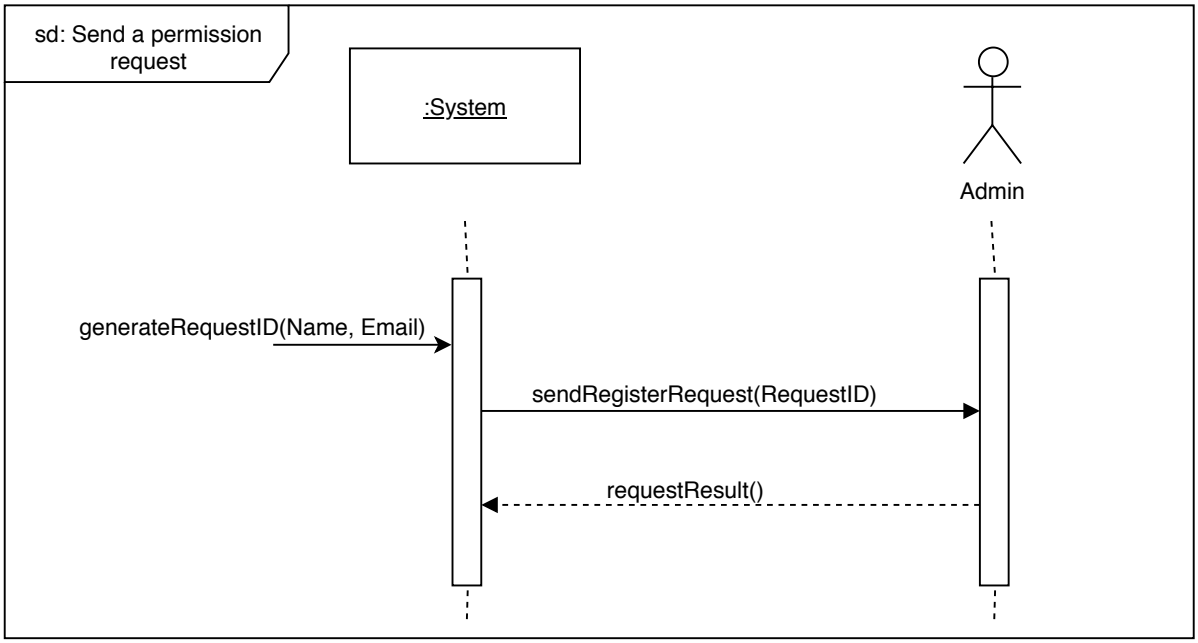
Team: The Straight A's

Register an account

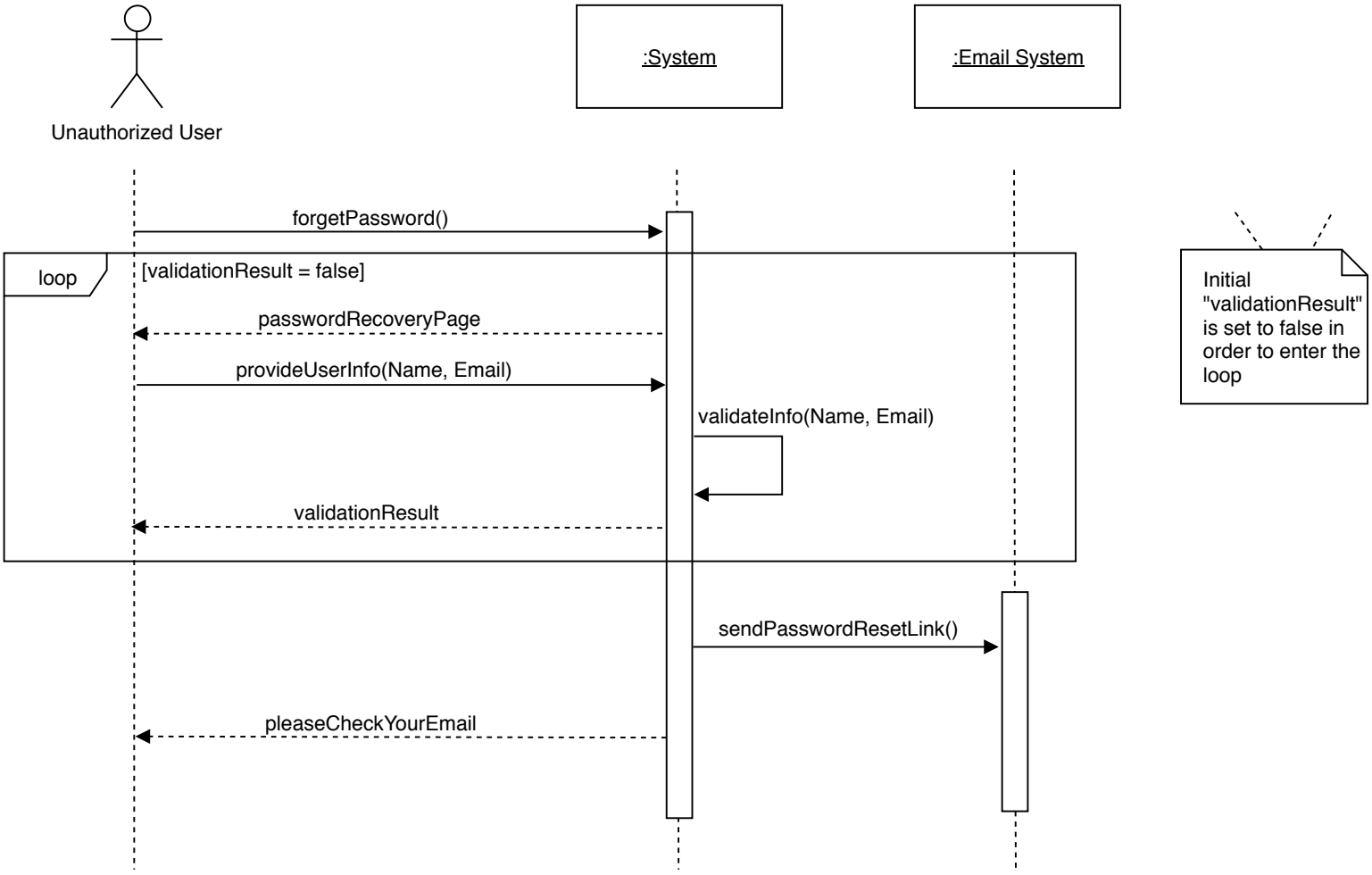



sd: Create new account
Unauthorized User
:System
loop
[validationResult = false]
generateAccountCreationPage()
Initial "validationResult" is set to false in order to enter the loop
providePersonalInfo(Name, Email, Username, Password)
validateInfo(Name, Email, Username, Password)
validationResult

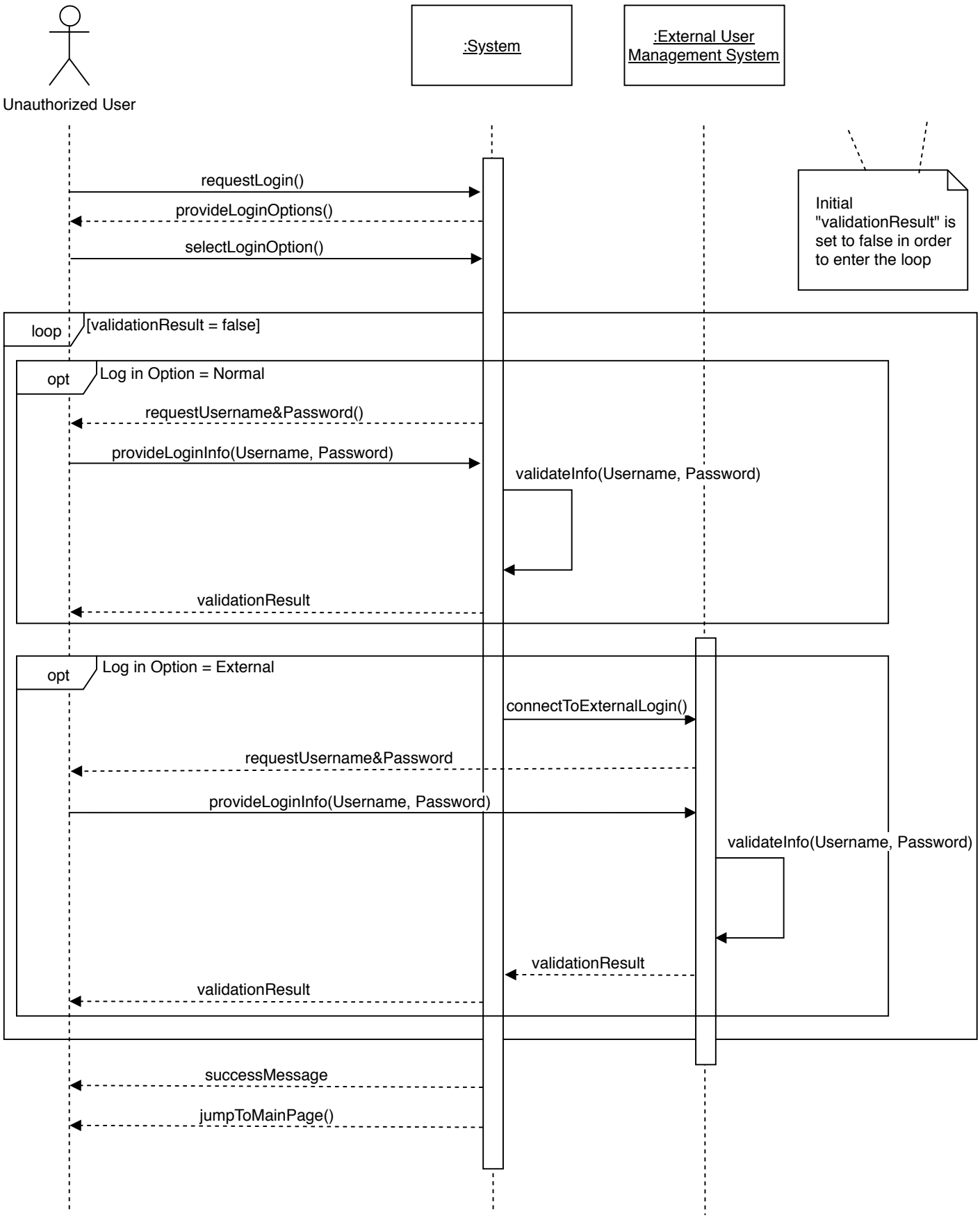

sd: Associate company/ organization account
Unauthorized User
:System
:External User Management System
Initial "validationResult" is set to false in order to enter the loop
loop
[validationResult = false]
externalLoginRequest()
generateLoginPage()
loginInfo(Username, Password)
validateInfo(Username, Password)
validationResult
validationResult
retrievePersonalInfo(Name, Email)
provideUserInfo



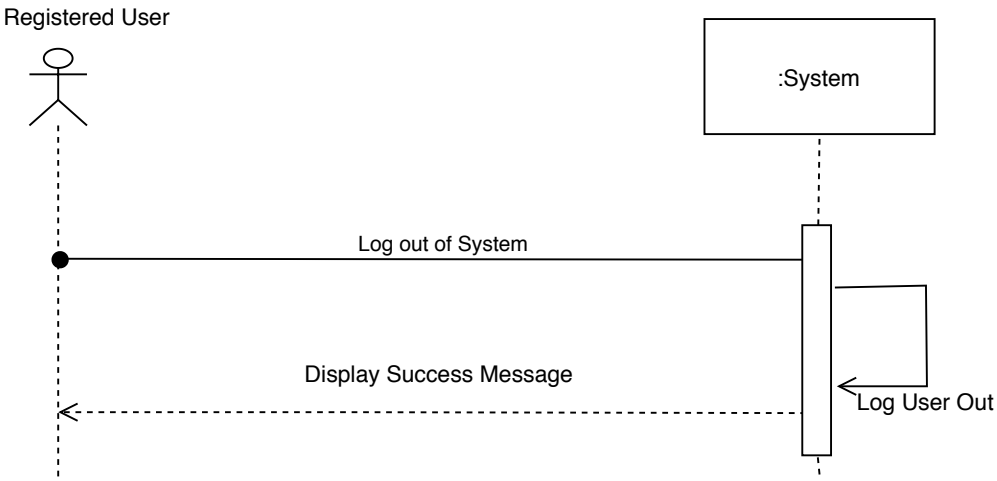
Password Recovery



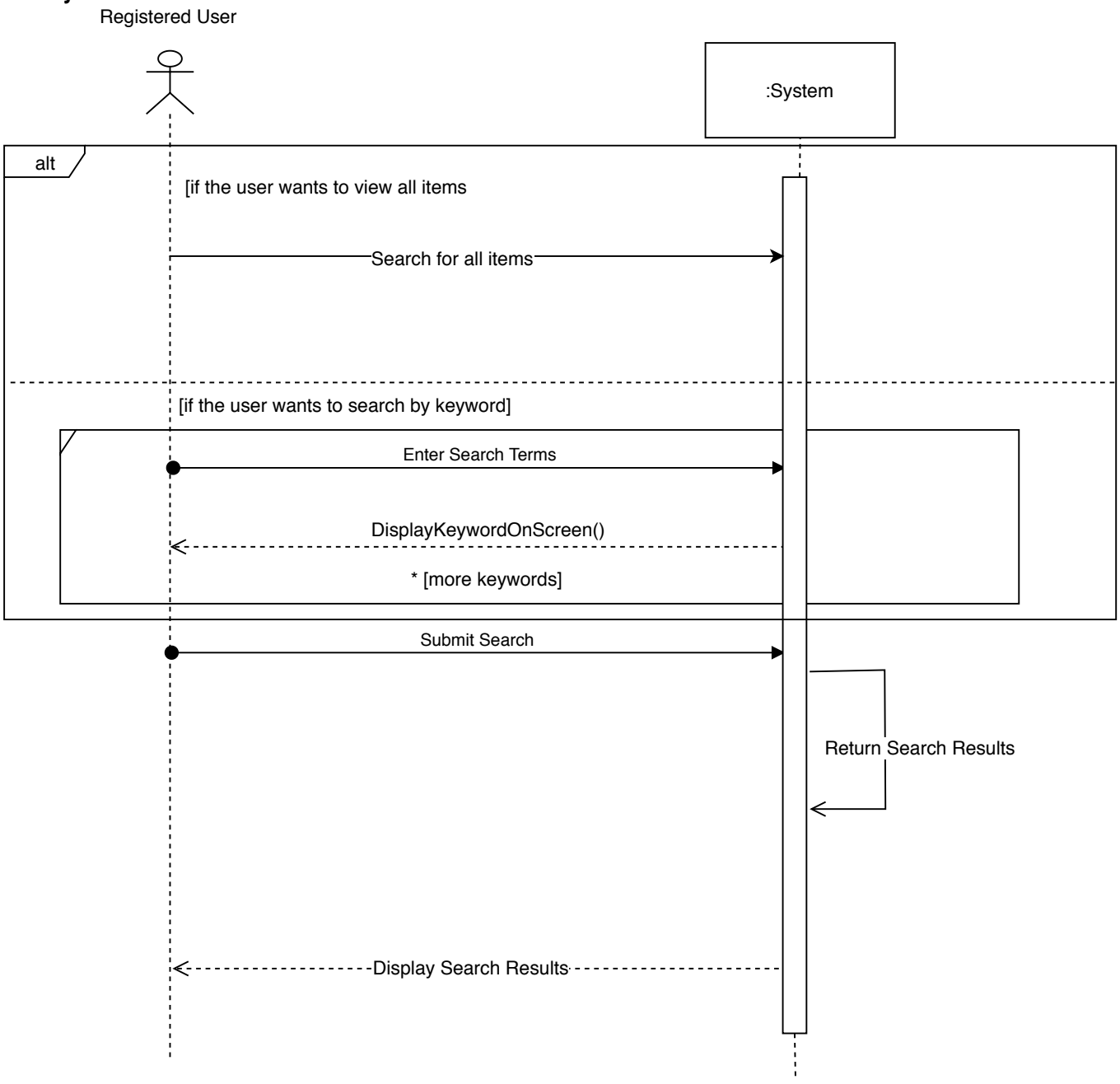
Log in


Unauthorized User
:System
:External User Management System
requestLogin()
provideLoginOptions()
selectLoginOption()
Initial "validationResult" is set to false in order to enter the loop
loop
[validationResult = false]
opt
Log in Option = Normal
requestUsername&Password()
provideLoginInfo(Username, Password)
validateInfo(Username, Password)
validationResult
opt
Log in Option = External
connectToExternalLogin()
requestUsername&Password
provideLoginInfo(Username, Password)
validateInfo(Username, Password)
validationResult
validationResult
successMessage
jumpToMainPage()

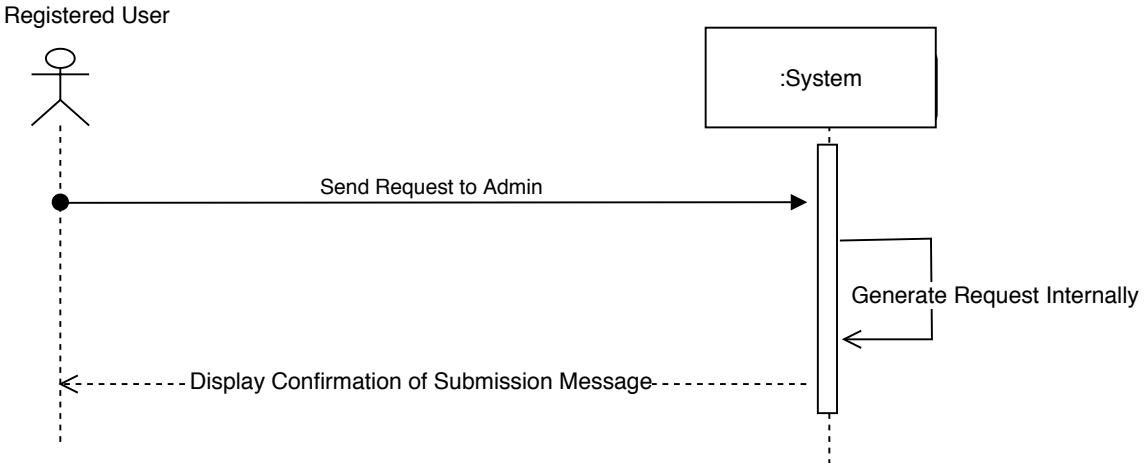
Log Out



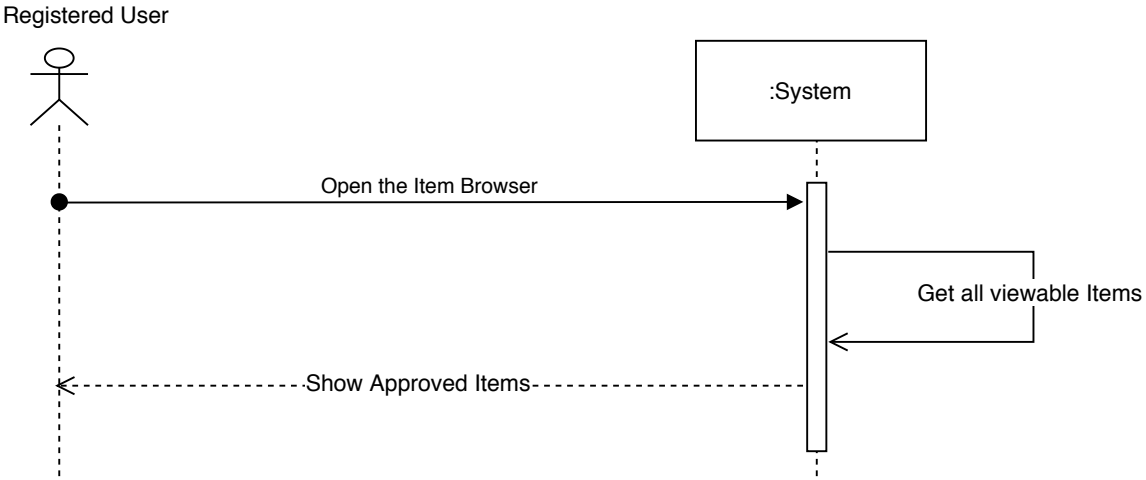
Search objects



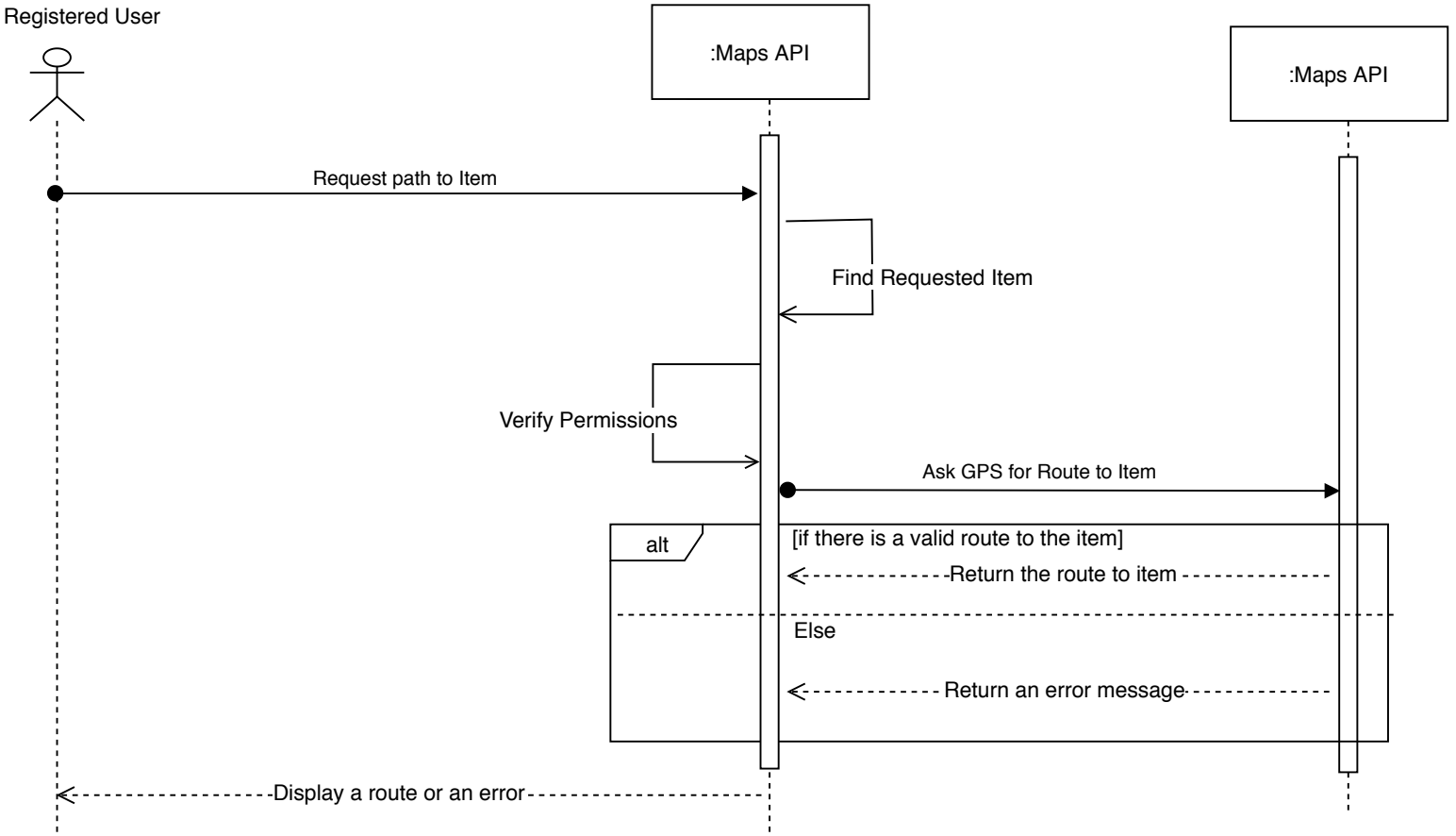
Send a General Request to the Admin



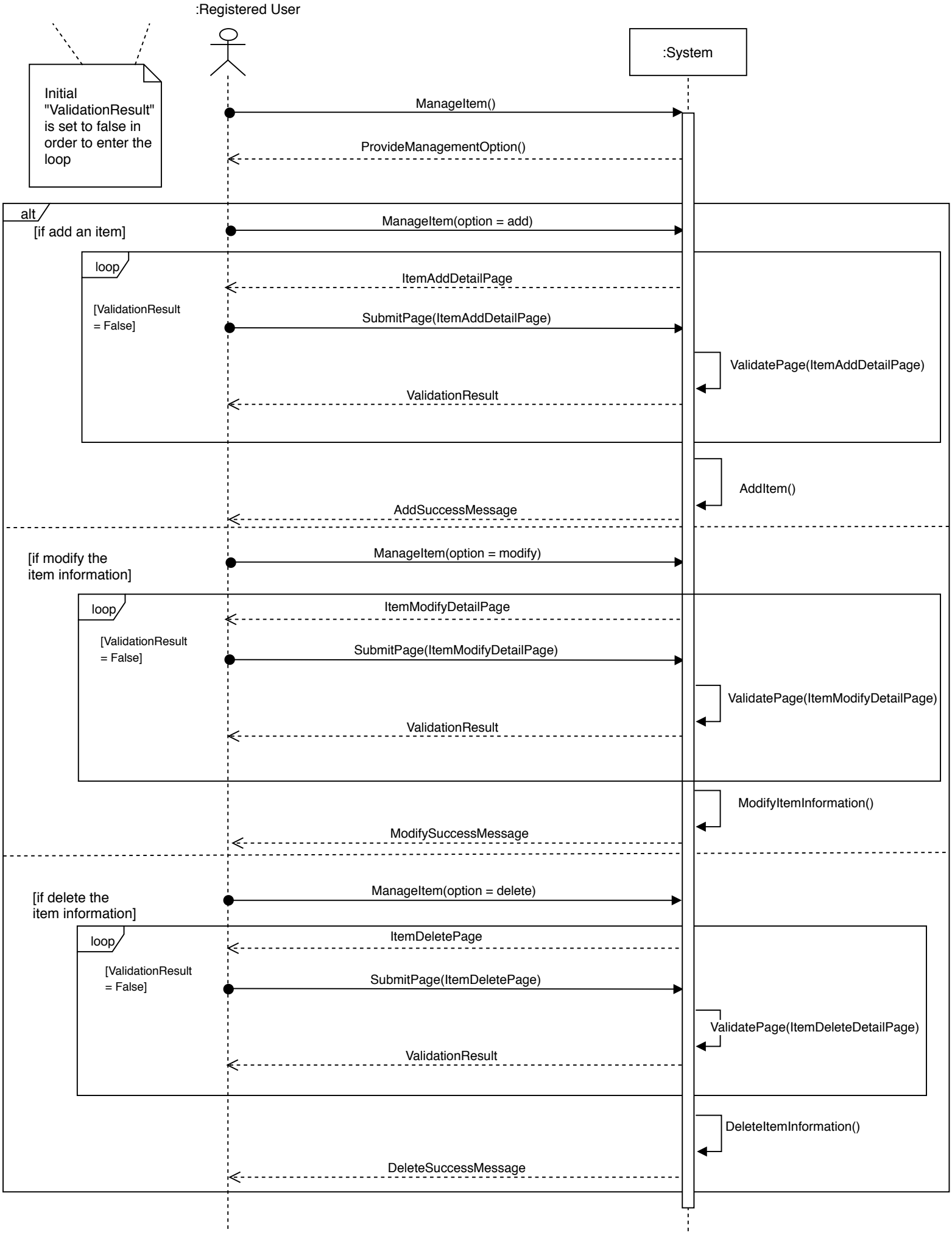
Browse objects



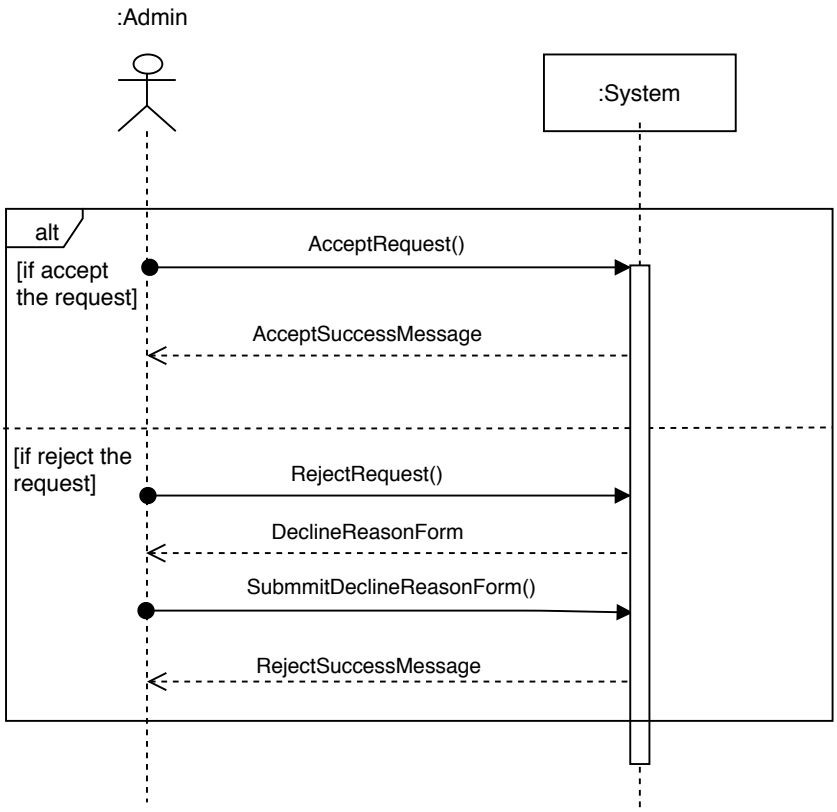
Navigate to Item



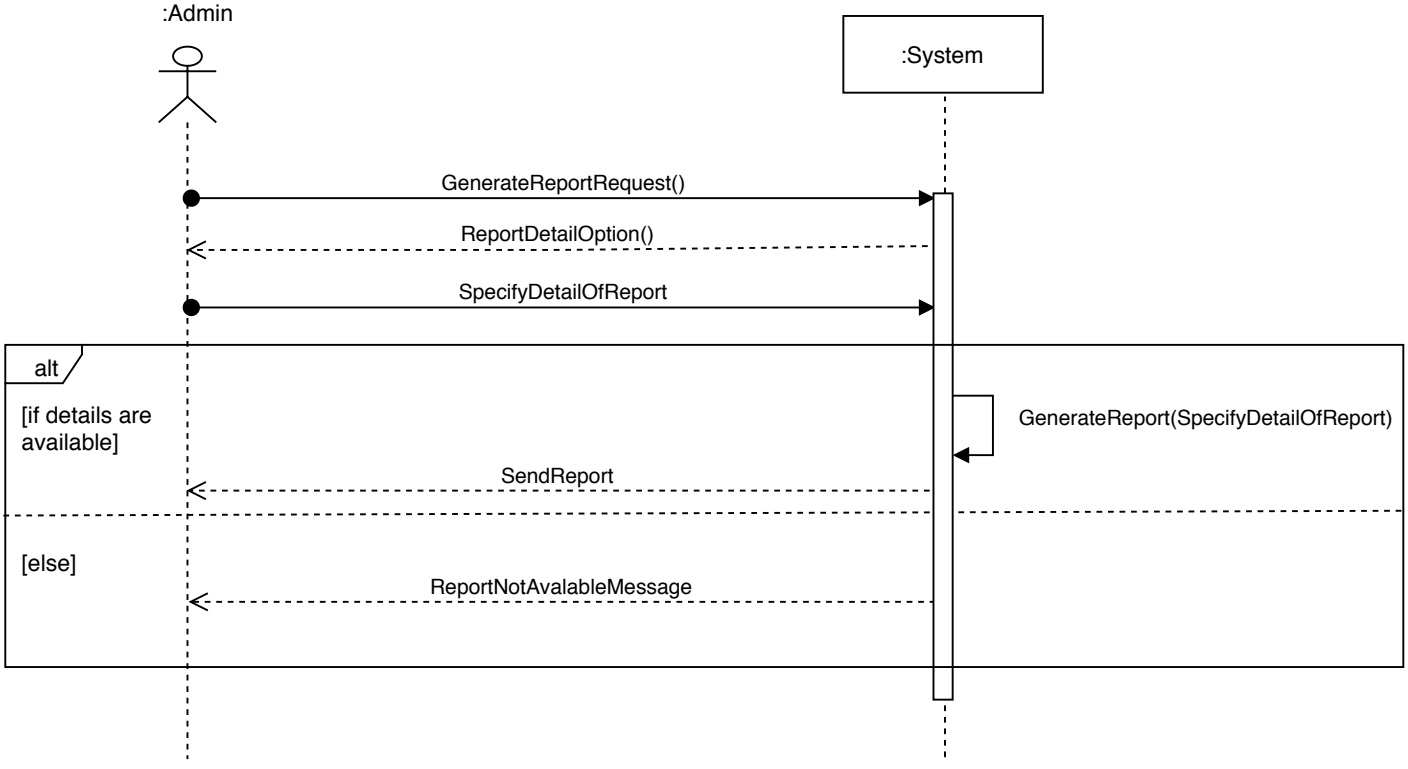
Manage items



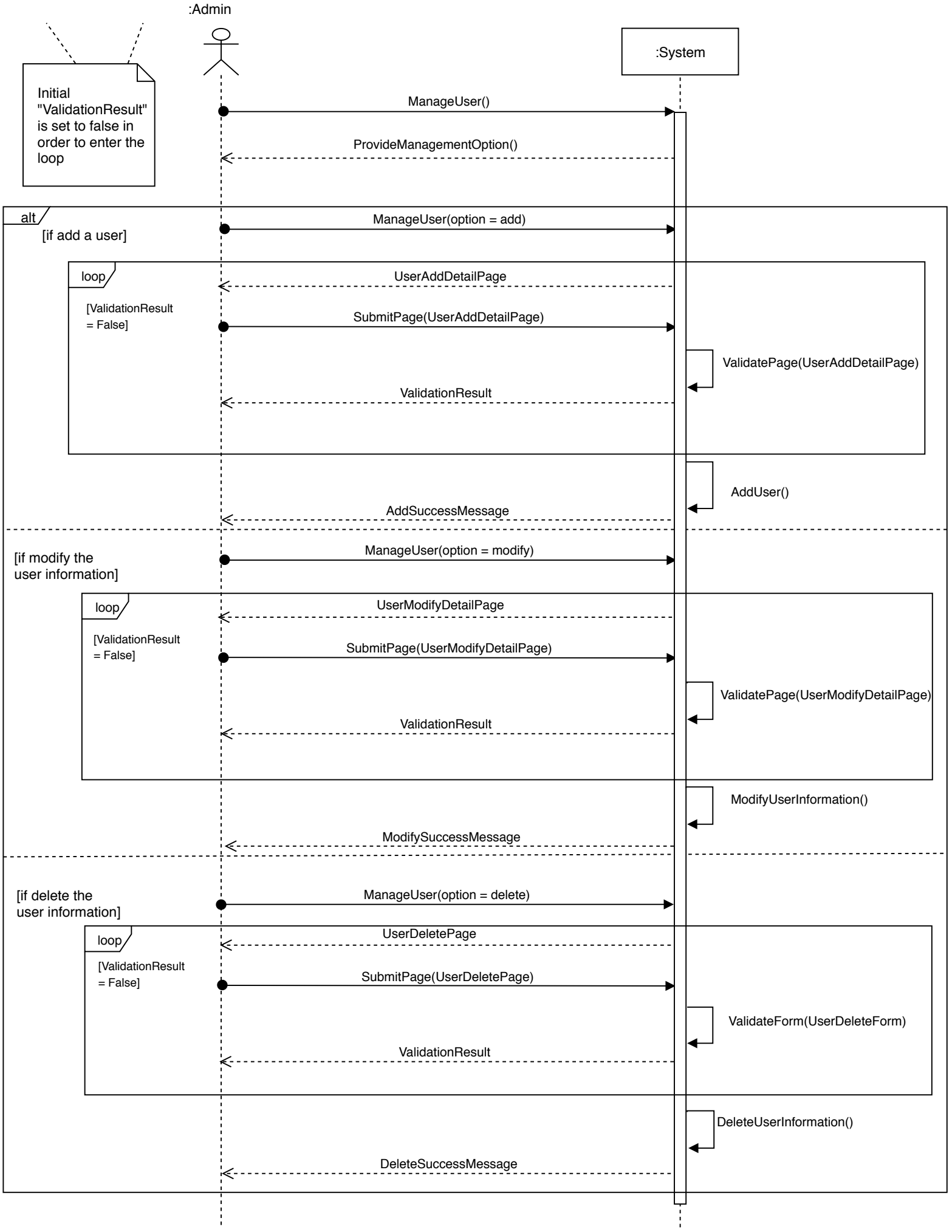
Approve/Reject User's Request



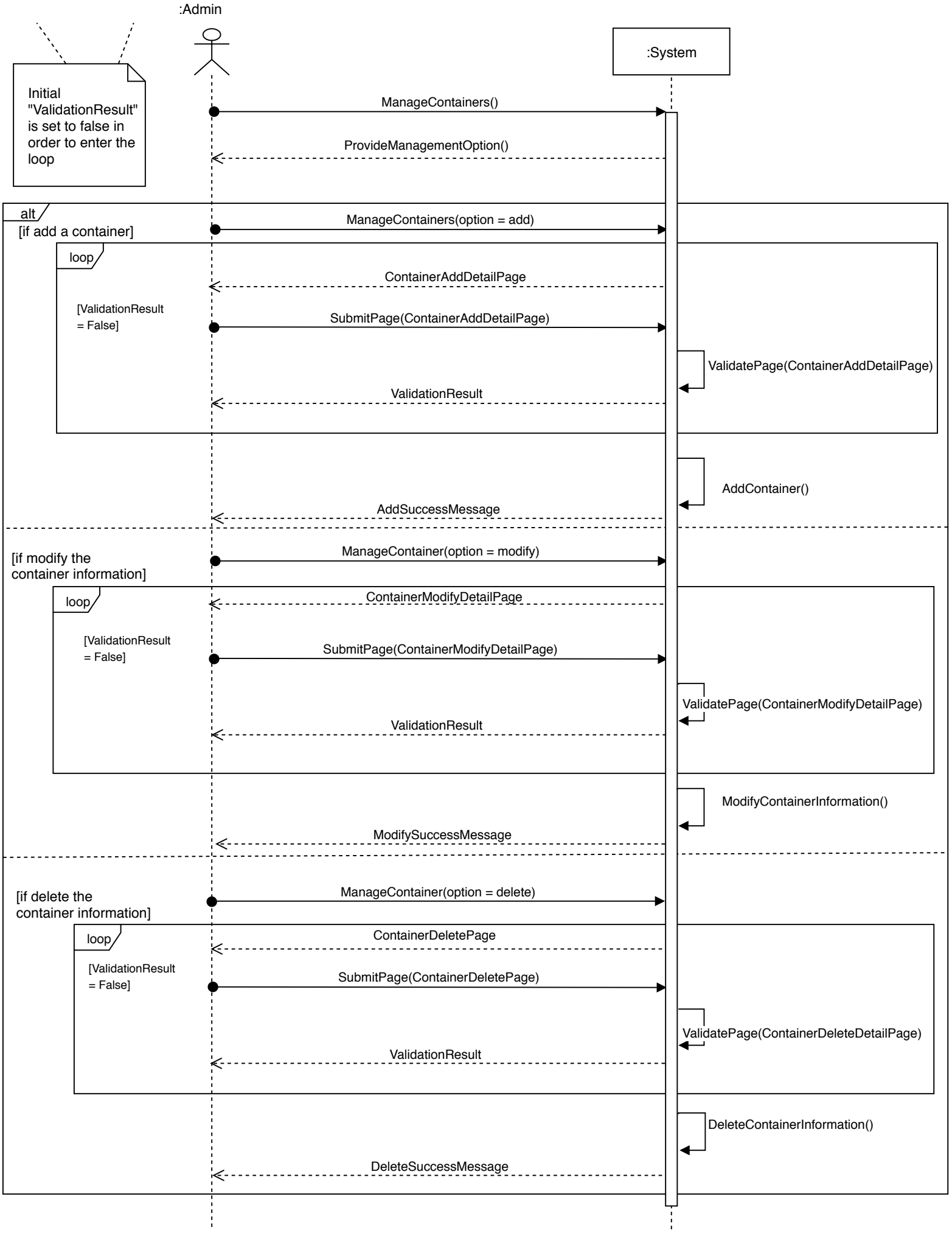
Generate Report



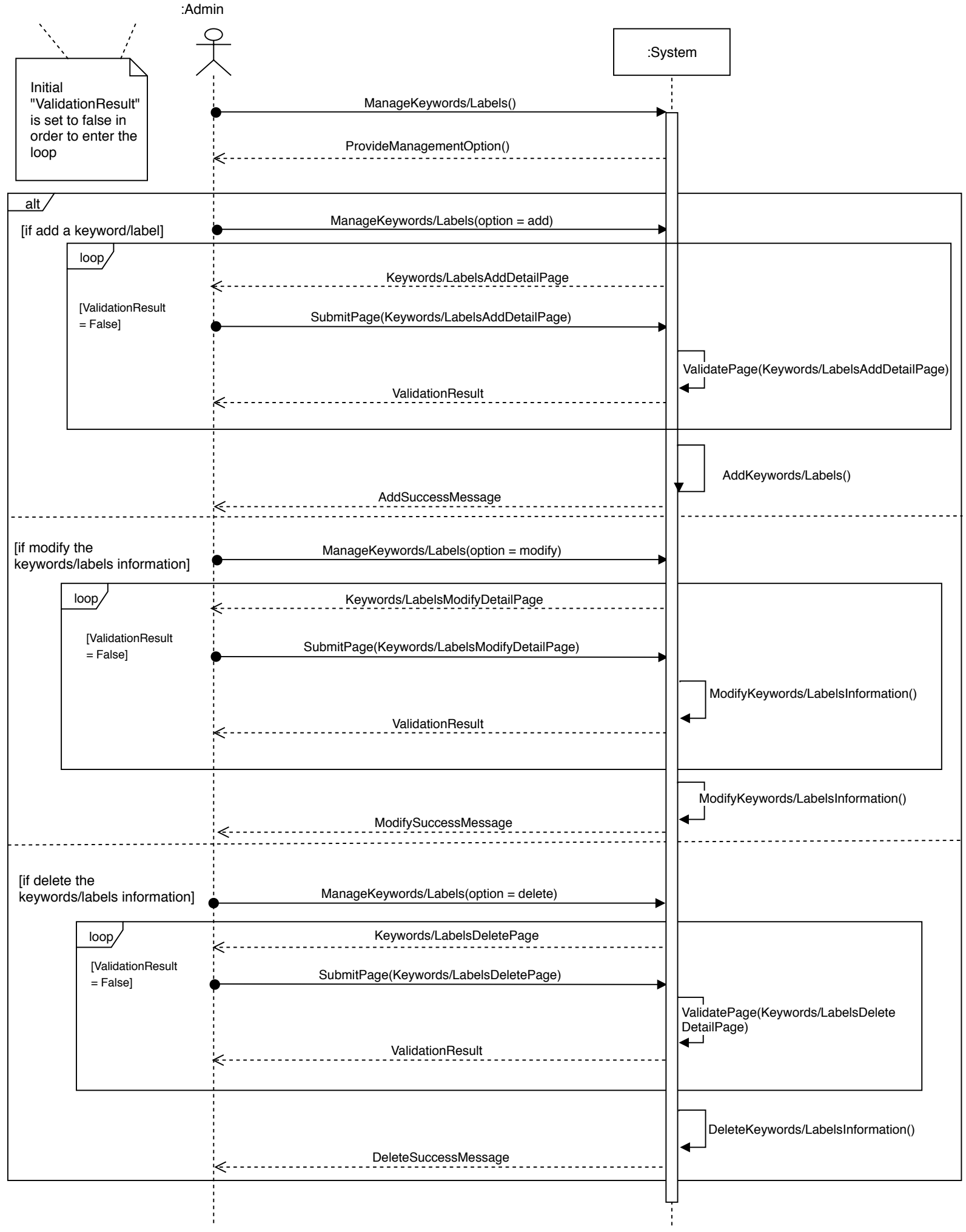
Manage User


:Admin
:System
Initial "ValidationResult" is set to false in order to enter the loop
ManageUser()
ProvideManagementOption()
alt
[if add a user]
ManageUser(option = add)
loop
[ValidationResult = False]
UserAddDetailPage
SubmitPage(UserAddDetailPage)
ValidatePage(UserAddDetailPage)
ValidationResult
AddUser()
AddSuccessMessage
[if modify the user information]
ManageUser(option = modify)
loop
[ValidationResult = False]
UserModifyDetailPage
SubmitPage(UserModifyDetailPage)
ValidatePage(UserModifyDetailPage)
ValidationResult
ModifyUserInformation()
ModifySuccessMessage
[if delete the user information]
ManageUser(option = delete)
loop
[ValidationResult = False]
UserDeletePage
SubmitPage(UserDeletePage)
ValidateForm(UserDeleteForm)
ValidationResult
DeleteUserInformation()
DeleteSuccessMessage

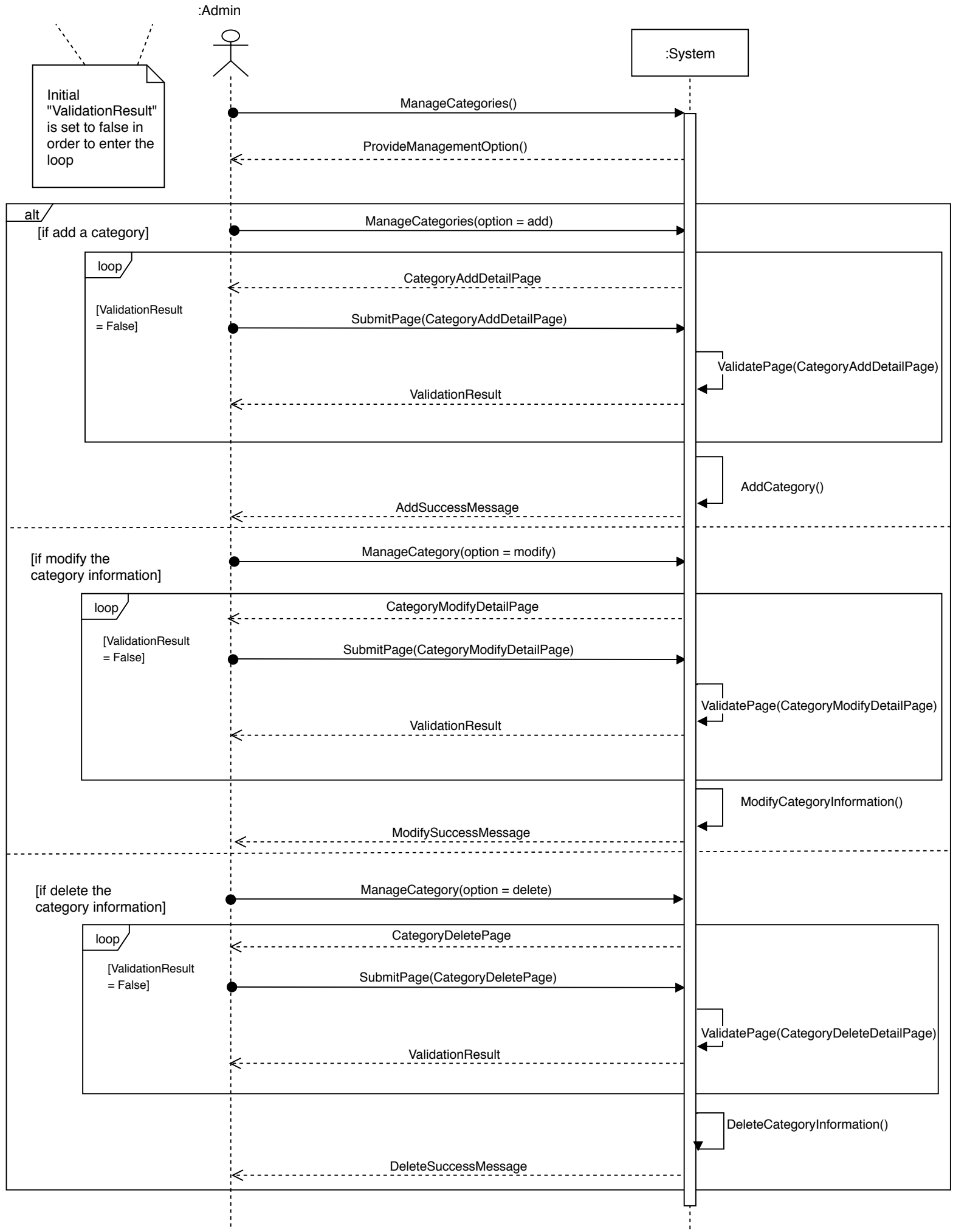
Manage containers



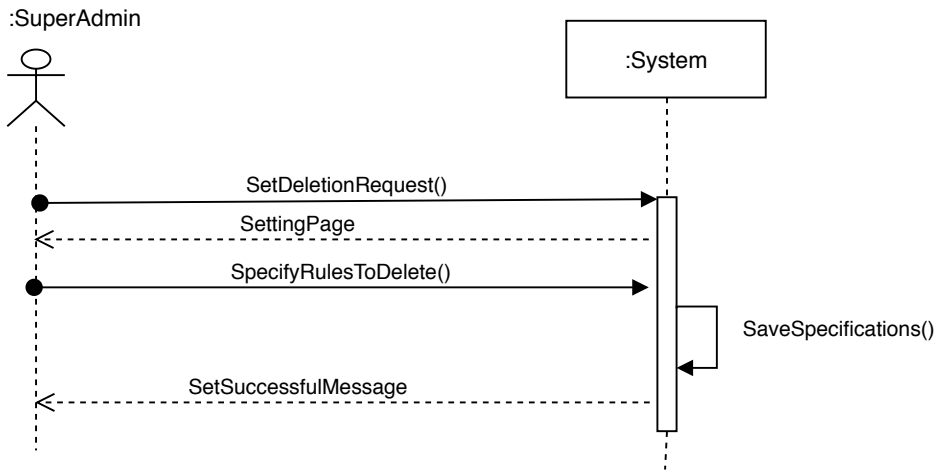
Manage Keywords/Labels



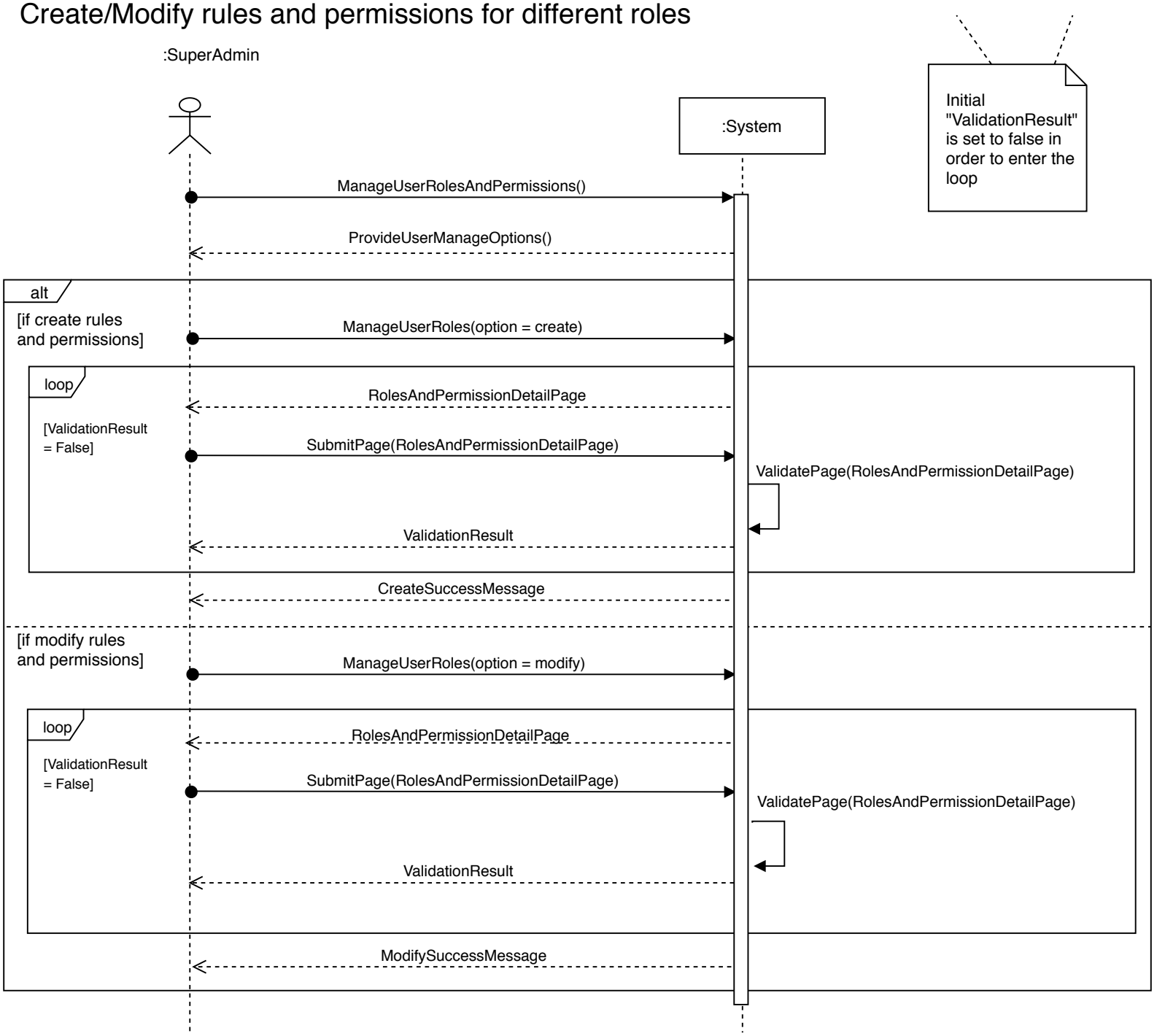
Manage Categories



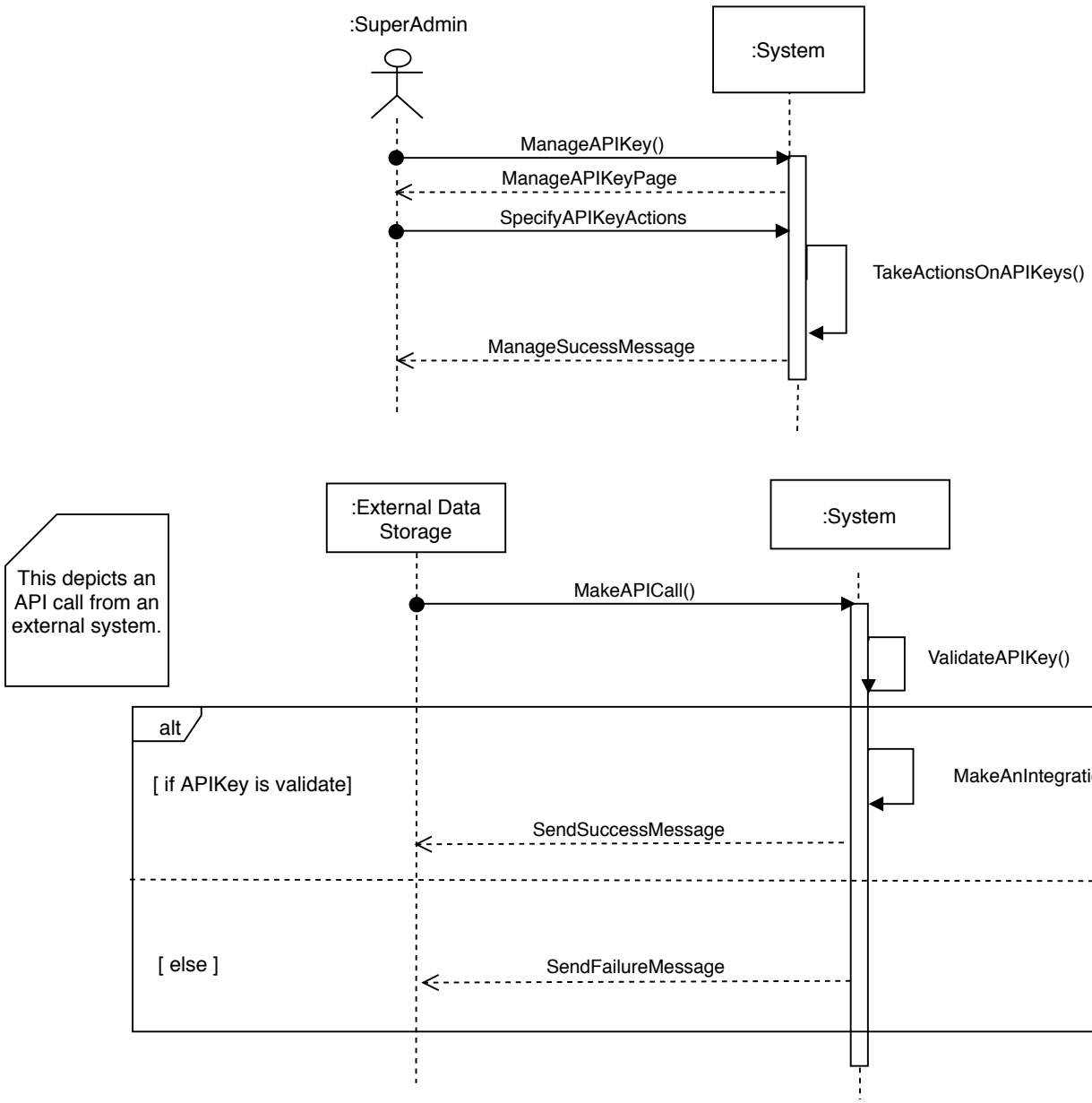
Deletion Control Management



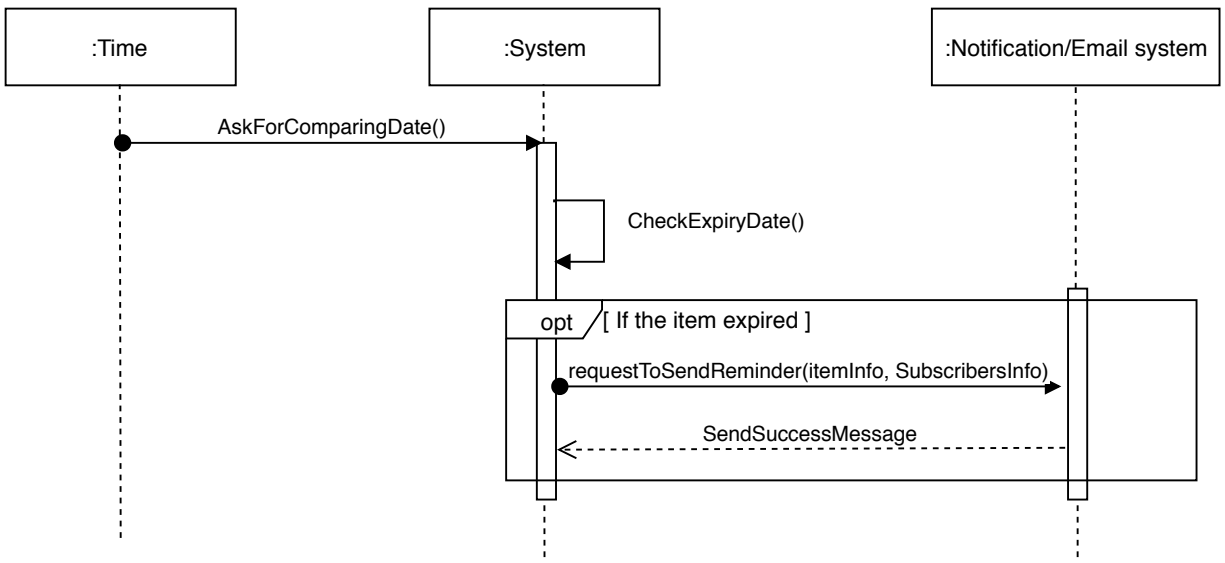
Create/Modify rules and permissions for different roles



Manage API Keys



Send notifications



e-Catalog Domain Model

Team: The Straight A's

Unauthorized User

Files

Registered User

Admin

Super-admin

Is Located At

Manages

Views

Contains

Receives

Has

Belongs to

Associated With

Approves or Rejects

Generates

Triggers

<<Shared Phenomenon>>
Container

name
description

<<Shared Phenomenon>>
Item

name
ID
description
checkedOut: Boolean
expiryDate: Date
action: {WarnUser, NoAction, RunCustomAction}

Utility Class

Date

Today: Date

= (d: Date): Boolean
< (d: Date): Boolean
- (d:date): Duration
date() : 1..31

<<Shared Phenomenon>>
Location

coordinates

<<Shared Phenomenon>>
User Profile

username
password
name
email

<<Shared Phenomenon>>
Item Expiry Notification

message

<<Shared Phenomenon>>
Category

name

<<Shared Phenomenon>>
User Request

requestID
requestDepartment
requestSubject
requestContent

<<Shared Phenomenon>>
Report

reportID
date: Date
title
content

<<Shared Phenomenon>>
API Key

APIKeyValue
intendedUserOrganization
intendedUserSystem
intendedUsageDescription

<<Shared Phenomenon>>
Action

triggeredOn: {NonEmptyContainerDeletion}
actionType: {WarnAndContinue, NoWarnAndContinue, CancelOperation}

<<Shared Phenomenon>>
Role

department
roleType: {RegisteredUser, Admin, SuperAdmin}

<<Shared Phenomenon>>
Permission

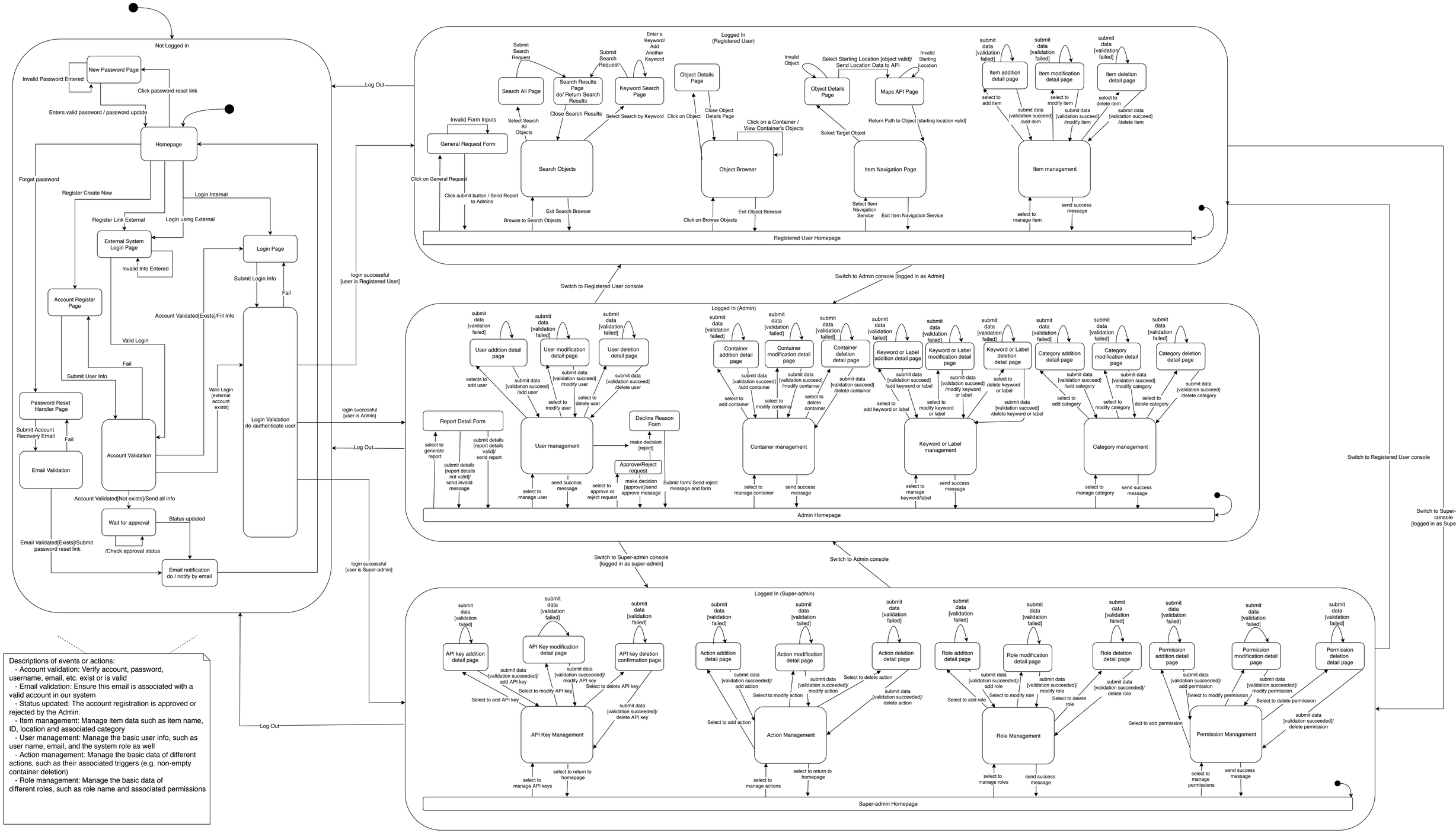
name
power

<<Actor>>
Time

Sets and Removes

e-Catalog State-Machine Model

Team: The Straight A's



Descriptions of events or actions:
- Account validation: Verify account, password, username, email, etc. exist or is valid
- Email validation: Ensure this email is associated with a valid account in our system
- Status updated: The account registration is approved or rejected by the Admin.
- Item management: Manage item data such as item name, ID, location and associated category
- User management: Manage the basic user info, such as user name, email, and the system role as well
- Action management: Manage the basic data of different actions, such as their associated triggers (e.g. non-empty container deletion)
- Role management: Manage the basic data of different roles, such as role name and associated permissions