COMP 225 - Software Engineering Methodologies

Software Requirements Specification (SRS)

Project Name : Graphical Passwords Software

Presented by

Group 8:

Jungyu Lee 301236221,

Manvibolreach Ouk 301224112

Date : August 12

Section #: 006

Semester : Summer 2022

Contents

Introduction

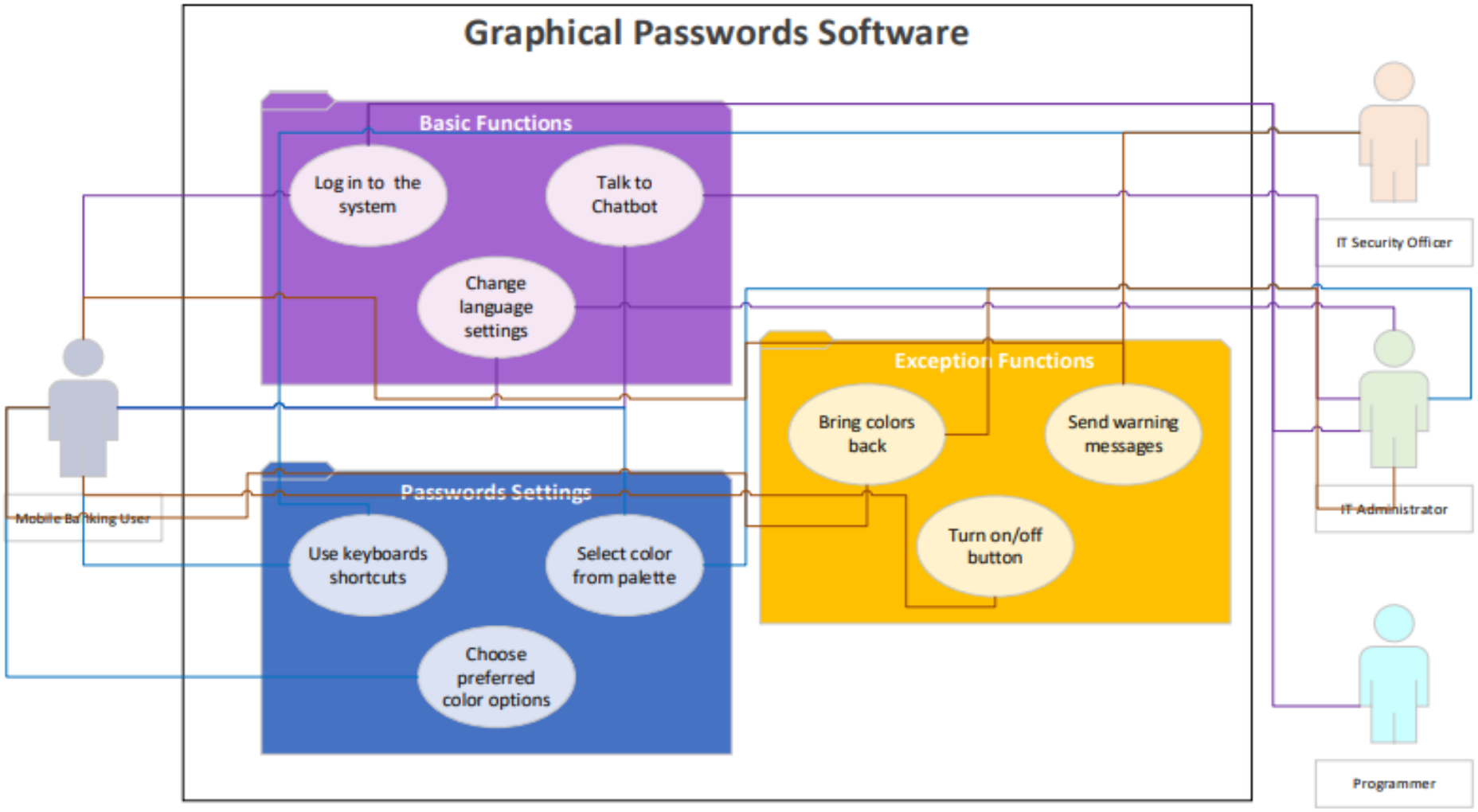
Purpose

- This new software product will solve the problem of securing users' personal information by preventing Shoulder Surfing. This is version 1.0.0.

Project Scope

- Many people are at risk of hacking when they access or store personal information in public places. It is a software that prevents them from the danger of hacking. By using this program, users can safely log in to any service in a public place. The software has the advantage of offsetting the concept of 'key' because it creates a combination of preset colors and numbers of colors. It can have color distortion software to create confusion for people who try shoulder surfing when viewed from a different direction. Keyboard shortcuts help reduce password entry time and increase security as traditional methods do. In particular, the secondary authentication number that comes through text messages when handling money-related tasks is also at risk of hacking, so that part can be prevented.

Packaged Use Case Diagram



Use Cases Brief Descriptions

Goal Use Case name	Actors	Use Case Brief Description
Select color from palette	Service Users, IT administrators	All service users will choose a specific color from the palette to set up the passwords at the beginning of the system. They will enter the passwords which will match the coordinates. This process is required for all service users to use the graphical password system. While the customer can choose colors from the palette, the color will be given as HSLA values to the IT administrators.
Log-in to the system	Service Users, IT administrators, Programmers	Log-in API is one of the most fundamental functions in the system. Therefore, it is required for all service users to use this system. Log-in API is connected with the graphical password software and allows the service users to enter user's information including the passwords. IT administrators will do the usual work to run the login API, and programmers will do the maintenance work if necessary.

Use Cases Brief Descriptions (Continued)

Goal Use Case name	Actors	Use Case Brief Description
Use keyboard shortcuts	Service Users, IT Security Officers	All service users will use keyboard shortcuts to enter the passwords. This is the core function in the graphical password system. A user will set their passwords combined with colors, letters, and numbers. Every time the user tries to enter the passwords, the graphical passwords software will offer random coordinates for passwords. The user can press keyboard shortcuts which are mapped with each coordinate. The user can customize his/her own shortcut key as well as simply using the default shortcut key. The algorithms for random coordinates must not be predictable and maintained regularly to provide the stable password security by IT security officers.

Use Cases Brief Descriptions (Continued)

Goal Use Case name	Actors	Use Case Brief Description
Turn on/off button	Service users	The graphical passwords system is optional, which means all service users can deactivate it, and use the traditional passwords system with the turn on/off button when necessary. Users can find this button at the top right of the corner of the screen. If they turn the button off, the system will disappear and provide traditional passwords log-in API. When they turn the button on, the system will show up and work again.
Change language settings	Service Users, IT administrators	All service users can change the language preferable to them. The graphical passwords software will present several languages such as English, Spanish, Arabic, et cetera. The users will select the preferred language. The software will automatically change the language for the manual, chatbot service, and guidelines, which will be managed and updated by IT administrators.

Use Cases Brief Descriptions (Continued)

Goal Use Case name	Actors	Use Case Brief Description
Choose preferred color options	Service users	All service users can set colors to their taste. They will click on the color option button. This function is going to be popular especially for the younger generation since it can show individuality. Furthermore, based on their selected colors, the colors will take turns every time the actor tries to log in, which will help enhance security.

Use Case Full Description

Use case	Use keyboard shortcut
Iteration	1, last modification: June 16, 2022
Primary actor	Mobile banking user
Goal in context	To enter passwords safely at a faster speed
Preconditions	The system must be fully configured. Initial passwords (a combination of colors, numbers, and letters) must be set by a user. Algorithms must be active to provide coordinates for passwords.
Trigger	The mobile banking user enters ID. The system recognizes the user's passwords matching the ID and provide the coordinates for passwords.

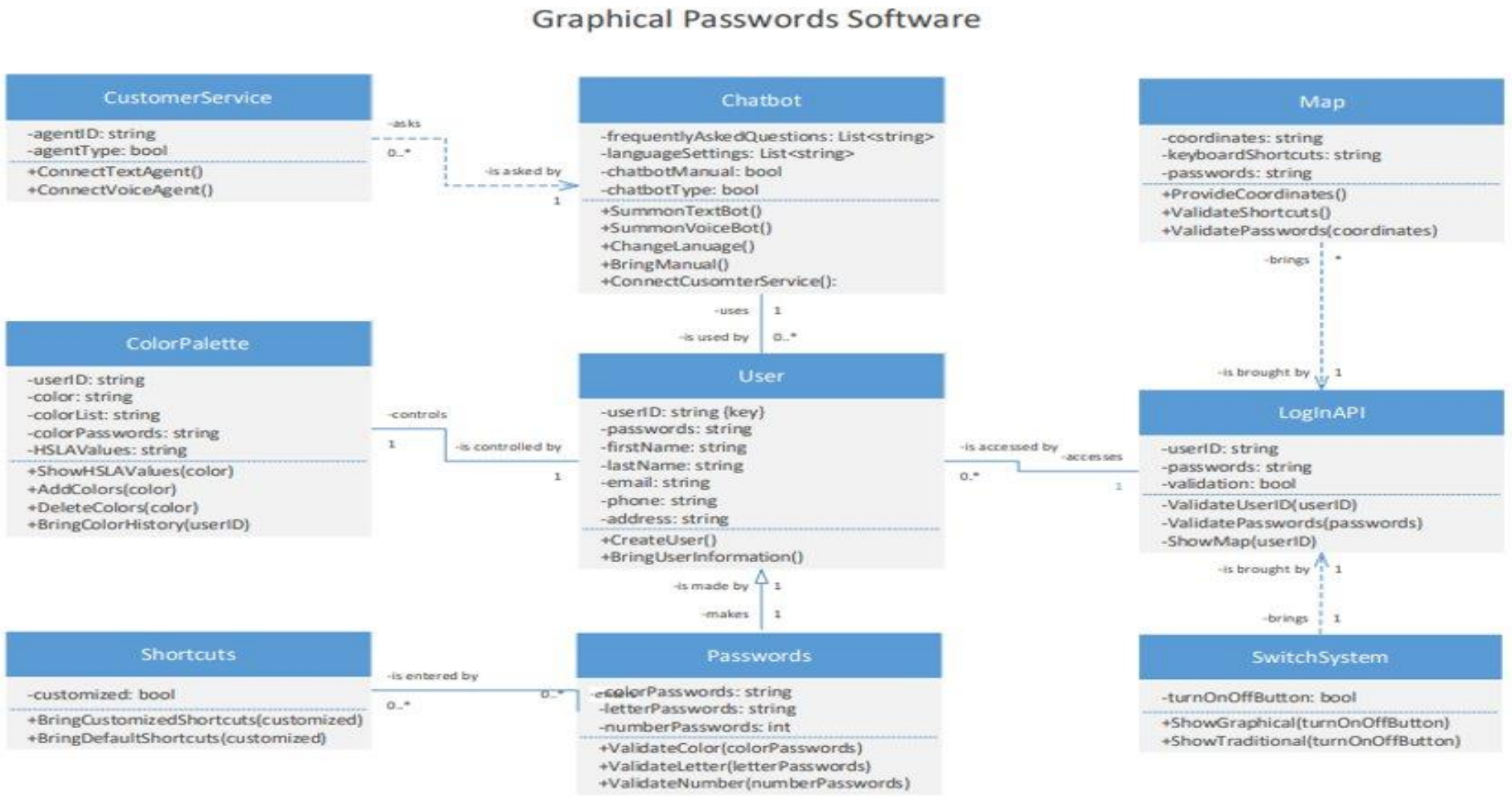
Use Case Full Description (Continued)

Scenario	1. The mobile banking user (the user) opens the banking app. 2. The user enters ID, and the server checks the ID. 3. The user is given the map for random colors, letters, and numbers from the server. 4. The user enters color coordinates that correspond the specific position on the map by using keyboard shortcuts. 5. The user enters letter coordinates that correspond the specific position on the map by using keyboard shortcuts. 6. The user enters number coordinates that correspond the specific position on the map by using keyboard shortcuts. 7. The user enters all the passwords and click on the log-in button. 8. The complete coordinates mapping with the user's passwords are delivered to the server. 9. The user logs in to the banking system successfully.
Exceptions	- The server detects shared networks or viruses on user's part. It sends warning messages to the user whether to proceed. - ID is incorrect. The user has to go through ID validation process. - Passwords are incorrect. The user is given three different maps to try, then has to go through passwords validation process. - The user can traditional password log-in system with turn on/off button – See Use Case Turn on/off button.

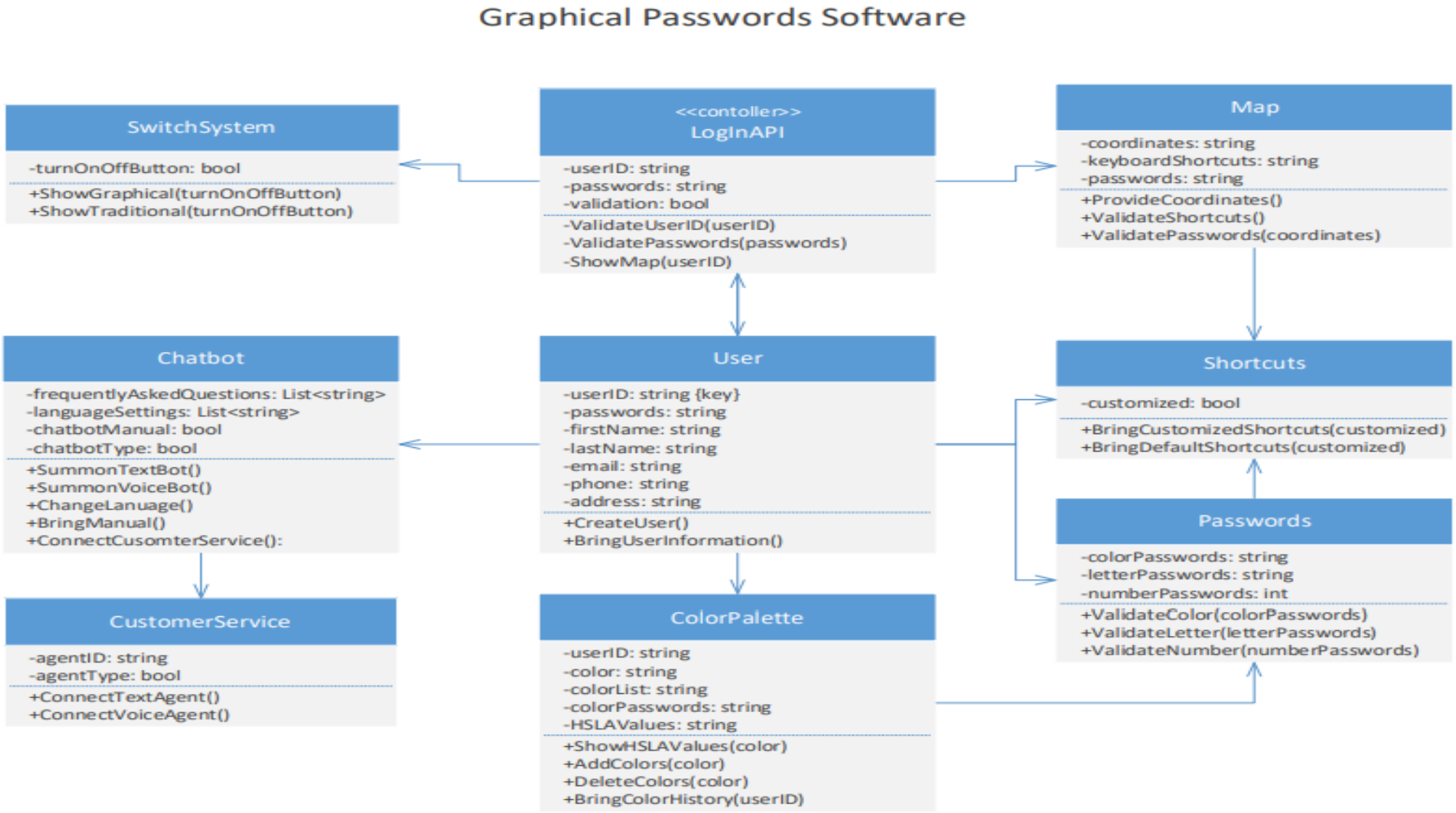
Use Case Full Description (Continued)

Priority	Highest, the core of the graphical password system
When available	Third Increment
Frequency of use	High
Channel to actor	Via PC-based browser, mobile-based browser, mobile application with Internet connection
Secondary actors	Server, IT security officers
Channels to secondary actors	Via PC-based browser, mobile-based browser, mobile application with Internet connection.
Open issues	- Is security sufficient? Hacking into the feature would represent a major invasion of privacy. - What mechanisms trigger the warning message system to protect the user? - How algorithms provide maps for coordinates, and is it enough and well-functioned?

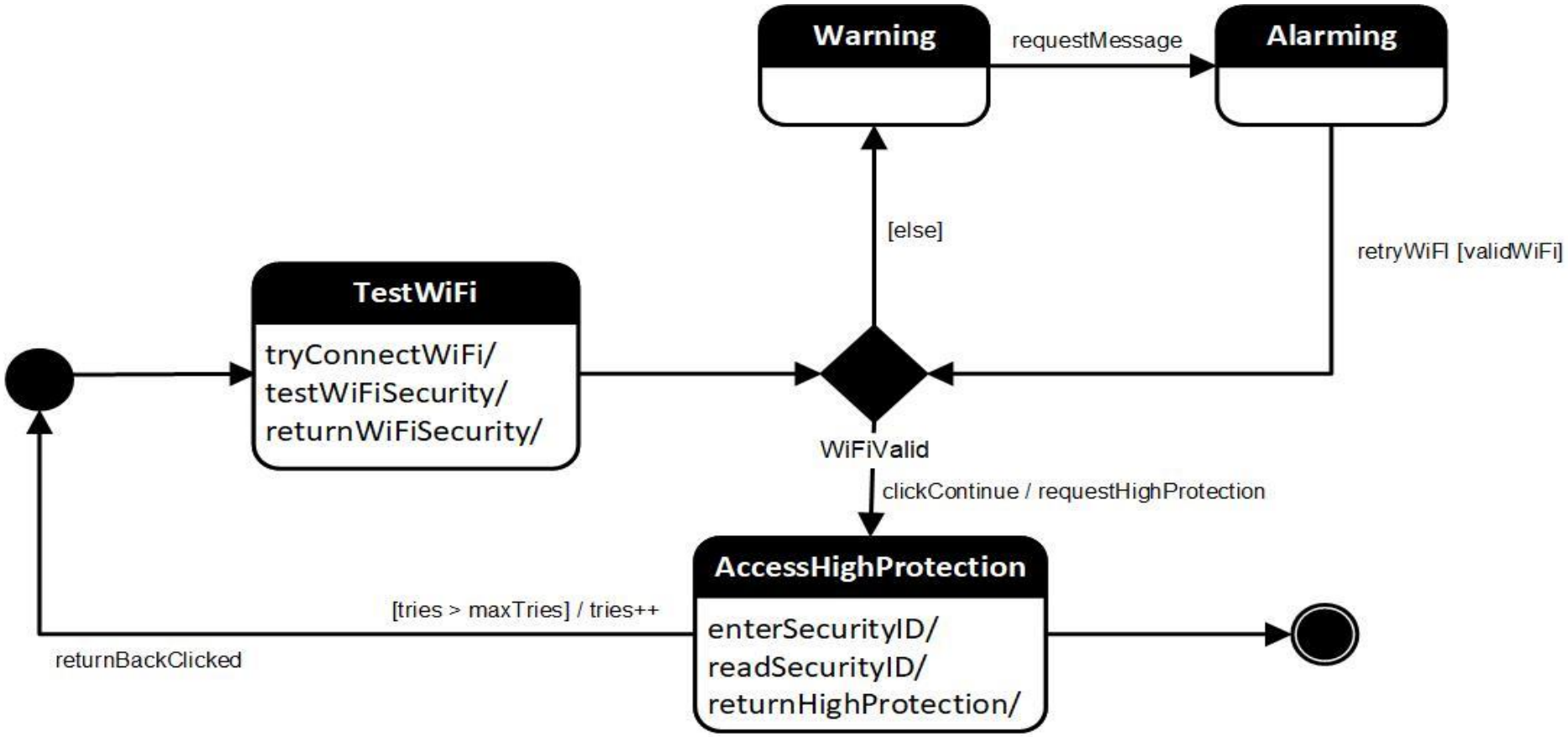
Domain Class Diagram



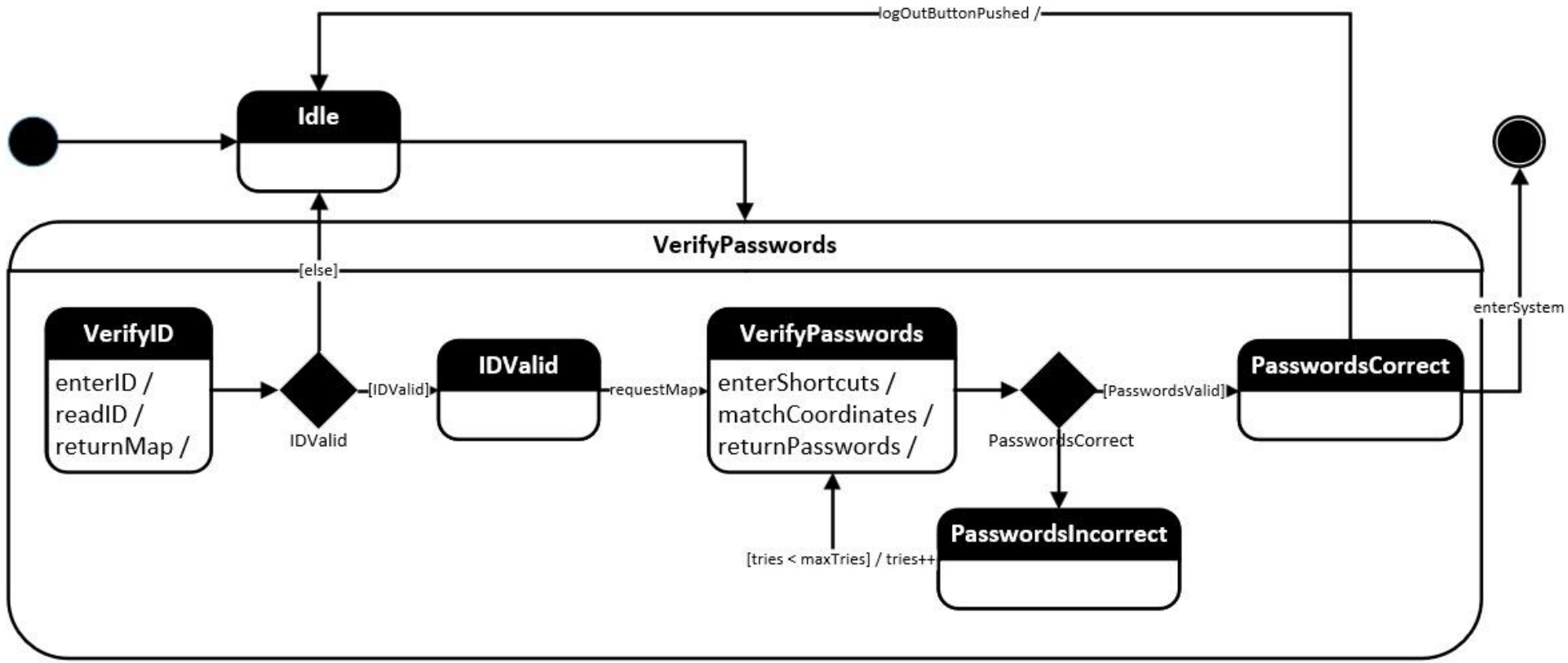
Updated First Cut Domain Class Diagram



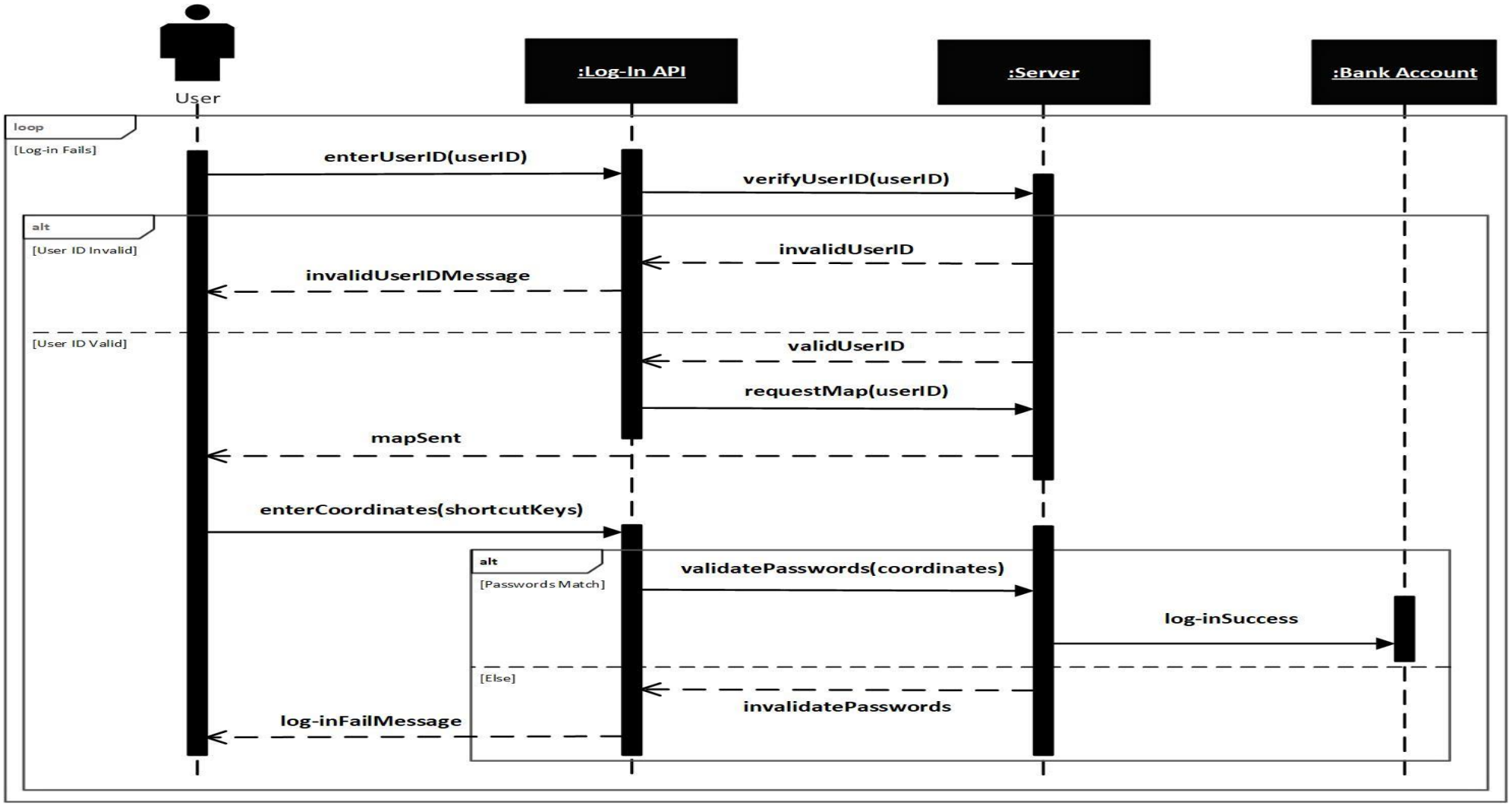
State Machine Diagram 1



State Machine Diagram 2



Sequence Diagram



Thank You