

Politecnico di Milano
AA 2017-2018

Computer Science and Engineering
Software Engineering 2 Project

Data4help

by TrackMe

RASD

Requirement Analysis and Specification Document

Tommaso Peresson – 845427
Giacomo Ziffer - 920905
Version 1.0 - 11/11/2018

SUMMARY

1	Introduction	3
1.1	Purpose.....	3
1.2	Scope	3
1.2.1	Description of the given problem	3
1.2.2	Goals	4
1.3	Definitions, Acronyms, Abbreviations	5
1.3.1	Definitions.....	5
1.3.2	Acronyms	5
1.4	Reference Documents	5
1.5	Document Structure.....	6
2	Overall Description.....	6
2.1	Product Perspective	6
2.2	Product Functions.....	6
2.2.1	Monitor location and health status of individuals.....	6
2.2.2	Send ambulance in case of emergency	7
2.3	User Characteristics.....	7
2.4	Constraints.....	7
2.4.1	Regulatory policies	7
2.4.2	Hardware limitations.....	8
2.4.3	Interfaces to other applications	8
2.5	Assumptions, Dependencies.....	8
2.5.1	Text assumptions	8
2.5.2	Domain assumptions.....	8
3	Specific Requirements	9
3.1	External Interface Requirements	9
3.1.1	User Interfaces	9
3.1.2	Hardware Interfaces	12
3.1.3	Software Interfaces	12
3.1.4	Communication Interfaces	12
3.2	Functional Requirements.....	13
3.3	Non-Functional Requirements	16
3.3.1	Performance	16

3.3.2	Reliability.....	16
3.3.3	Security	17
3.3.4	Scalability	17
3.3.5	Accuracy	17
4	Scenarios.....	17
4.1	Scenario 1	17
4.2	Scenario 2.....	17
4.3	Scenario 3.....	18
4.4	Scenario 4.....	18
4.5	Scenario 5.....	18
4.6	Scenario 6.....	18
5	Uml modelling.....	19
5.1	Use case descriptions	19
5.1.1	Visitor registration as a Private Customer	19
5.1.2	Visitor registration as a Business Customer	20
5.1.3	Accepting Business Customer's requests of subscription to Data4Help	21
5.1.4	Private Customer's subscription to AutomatedSOS	22
5.1.10	Private Customer reviews personal data.	25
5.1.11	AutomatedSOS: Emergency	25
5.2	Use case diagrams	26
5.2.1	Use case visitor and system manager.....	26
5.2.2	Use case Business and Private customers.....	27
5.3	Class diagram	28
5.4	State chart diagram.....	28
5.5	Sequence diagram	29
5.5.1	Request of anonymized data	29
5.5.2	Request for individual data	30
5.5.3	Business Customer registration.....	31
5.5.4	Business Customer registration approval.....	32
6	Formal analysis using Alloy	33
6.1	Alloy results	38

1 INTRODUCTION

1.1 PURPOSE

This document represents the Requirements Analysis Specification Document (RASD) for Data4Help and for AutomatedSOS, the two services that must be developed for TrackMe company. The purpose of this document is to describe the requirements of this system (both functional and non-functional), to identify its main goals and the users that will mainly interact with it. This document also analyzes the properties of the domain in which the system will be used and the constraints that have to be respected. The main application scenarios are analyzed to clearly explain the typical use cases that will occur after the release.

This document is intended for customers and users of the services, for systems and requirements analysts, developers, testers and project managers.

1.2 SCOPE

1.2.1 Description of the given problem

The purpose of the project is to develop a software-based service allowing third parties to monitor the location and health status of individuals.

By providing a simpler and more convenient way to communicate health data, the purpose of Data4Help is to offer a service that closes the gap between the doctors and patients and even facilitates research and analysis by third parties. A simple to use application will be distributed to all patients (from now on called Private Customers) through which Data4Help will be able to collect their personal health data that will be stored and processed. Afterwards the intent is to be able to offer this data, following all privacy concerns, to doctors and researchers (called Business Customer) to improve the reach and precision of their studies and diagnosis.

In order to exploit fully the capabilities of this platform Data4Help is interested also in release a sub-service called AutomatedSOS to provide immediate help to people in serious health conditions, by sending to the location of the customer an ambulance, when the parameters are below the threshold.

1.2.2 Goals

- [G1] Allow a Visitor to become a Private Customer.
- [G2] Allow a Visitor to become a Business Customer.
- [G3] Allow a Private Customer to subscribe to AutomatedSOS.
- [G4] Allow a Private Customer to review personal data.
- [G5] Allow a Business Customer to monitor data from Data4Help.
 - [G5.1] Allow a BC to monitor the real time position and the health status of a PC.
 - [G5.2] Allow a BC to monitor anonymized data about PCs' health status.
- [G6] Allow a Business Customer to request data from Data4Help.
 - [G6.1] Allow a BC to request the real time position and the health status of a PC.
 - [G6.2] Allow a BC to request anonymized data about PCs.
- [G7] Allow a Private Customer to share his real time position and health status with a Business Customer.
- [G8] Allow a Business Customer to subscribe to a data source like a specific PC or a geographical area.
- [G9] Allow a PC in serious health conditions to receive an ambulance in the shortest possible time.
- [G10] Allow a System Manager to do operations of system maintenance.
 - [G10.1] Allow a SM to verify and accept the request of appliance from a BC.

1.3 DEFINITIONS, ACRONYMS, ABBREVIATIONS

1.3.1 Definitions

- Private Customer: a customer that applies to the service Data4Help as a provider of personal health data and that can subscribe to AutomatedSOS
- Business Customer: a customer that applies to the service Data4Help as a user of the data acquired. It can be a single individual, such as a doctor, but also a company
- Anonymized Request: request made by a business customer, who asks for data grouped according to different possible parameters (i.e. place, age, etc.)
- Individual Request: request made by a business customer, who requests data belonging to a specific private customer, in this case the request must be accepted by the pc.

1.3.2 Acronyms

- [BC] as Business Customer
- [PC] as Private Customer
- [SSC] as Social Security Number
- [CF] as Codice Fiscale
- [SM] as System Manager
- [Gn]: n-goal.
- [Dn]: n-domain assumption.
- [Rn]: n-functional requirement.

1.4 REFERENCE DOCUMENTS

- Specifications Document: “Mandatory Project Assignment AY 2018-2019”
- IEEE Std 830-1998 “IEEE Recommended Practice for Software Requirements Specifications”

1.5 DOCUMENT STRUCTURE

The first section is an introduction. Its purpose is to provide a brief overview of the function of the system and the reasons for its development, its scope, and references to the development context. This introduction also includes the objectives of the project.

The second section presents an overall description of the project, including details on the shared phenomena and the domain models. The required functions are more precisely specified, with respect to the goals of the system, as well as the types of actors that can interact with the system.

The third part contains interface requirements, including: user interfaces, hardware interfaces, software interfaces and communication interfaces. This section analyzes even the requirements, from the domain properties to functional and non-functional requirements. The functional requirements are defined by describing few scenarios and by using sequence diagrams and use cases.

The fourth section includes the alloy model and the discussion for its purpose. A world generated by it is shown.

The fifth section shows the effort spent by each group member that worked on this document.

The sixth section shows the reference documents.

2 OVERALL DESCRIPTION

2.1 PRODUCT PERSPECTIVE

The product will be completely developed from scratch and will be composed of two components: the first is intended to be a web application, whose purpose is to interface with Business Customer, the latter is intended to be a smartphone application that will be used from the Private Customer. All data required for TrackMe for monitoring and analysis will be provided via a wearable device.

2.2 PRODUCT FUNCTIONS

In the following section, the functions of the system are listed and more precisely specified, with respect to the goals mentioned in section 1.2.

2.2.1 Monitor location and health status of individuals

After registration:

- Business Customers can access to the data of some specific individuals (by providing his/her social security number or his/her fiscal code in Italy). In this case, Data4Help passes the request to the specific individuals who can accept or refuse it.
In this case, BC can request real-time data or historical data of the specific user.

- Business Customers can access to anonymized data of groups of individuals (for instance, all those living in a certain geographical area, all those of a specific age range, etc.). In order to avoid a possible misuse of these data, these requests are handled directly by Data4Help that approves them if the number of individuals whose data satisfy the request is higher than 1000.
- Using the application, Private Customers can monitor their health status in real time, they can consult all the previously collected data and can also accept or reject requests from business customers who want to have access to their data.

The BC also has the option of requesting a subscription to a particular set of data, indicating the periodicity with which he/she wants the data to be updated. In this way, the BC will have at his/her disposal periodically the updated data required. Before any update, TrackMe will be obviously charged to check that the data always respect the parameters listed above (in the case of an anonymous group number of individuals higher than 1000), in the event that this condition is not met, the update will not be made available.

2.2.2 Send ambulance in case of emergency

By having real-time information on the health status of its private customers, TrackMe is able to know when they are in danger (some parameters fall below certain thresholds) and automatically calls an ambulance, through a prerecorded message, within 5 seconds from when the parameters have dropped below the threshold value.

2.3 USER CHARACTERISTICS

The following actors are the user of the application:

- *Visitor*: a person who is not registered yet in the service. The only thing he/she can do is proceeding with registration
- *Business Customer*: a person or a company passed through a successful registration process and now able to use the Data4Help service
- *Private Customer*: a person passed through a successful registration process and now able to review his/her data by using the app and can use AutomatedSOS
- *System Manager*: an employee of TrackMe able to maintain and update the system. He/she does not have to register, since he/she is added during system's installation process

2.4 CONSTRAINTS

2.4.1 Regulatory policies

The system will require billing information from users subscribed to paid services, that will be stored securely and used according to the service terms and conditions. All personal data will be kept private and, in any circumstance, will be sold to third-party. In order to render aware, the user of the fact that all his personal data will be stored on Data4Help's servers, during the registration procedure it will be forced to read a clear and concise document containing all privacy information.

2.4.2 Hardware limitations

- Mobile app
- IOS/Android Smartphone.
- 2G/3G/4G connection.
- GPS

2.4.3 Interfaces to other applications

In the first release the service will not export any interface to third-party applications.

2.5 ASSUMPTIONS, DEPENDENCIES

2.5.1 Text assumptions

- We assume that Data4Help is free for Private Customers.
- We assume that Data4Help is a paid service for Business Customers.
- We assume that AutomatedSOS is a paid service for Private Customers.
- We assume that if an anonymized data subscription interests less than a 1000 people it's automatically suspended until the number goes back above the threshold.

2.5.2 Domain assumptions

[D1] The device used by the user is able to provide accurate data on his/her health status.

[D2] The device used by the user is able to provide accurate data on his/her location.

[D3] The application has access to emergency numbers to call in case of emergency.

[D4] There is an external service that will be in charge of the payment information validity and the secure payment transactions.

[D5] All information entered by the user during registration in the service is correct.

[D6] GPS signal and 4G signal must always be available.

[D7] A system manager has technical knowledge in order to find inconsistencies in the Business Customer information.

[D8] The Wearable device is always paired with the Private Customer's phone.

[D9] All the health information is always available through OS API's.

3 SPECIFIC REQUIREMENTS

3.1 EXTERNAL INTERFACE REQUIREMENTS

3.1.1 User Interfaces

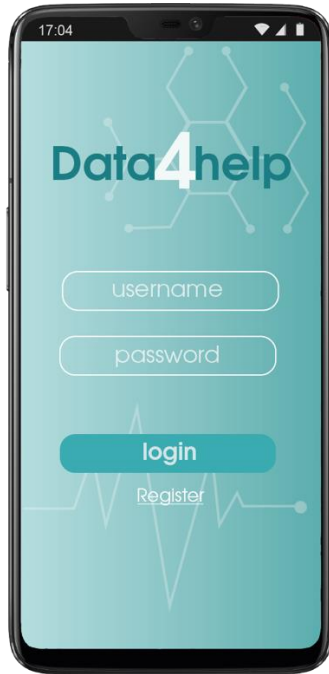


Figure 1 Log in / Sign up screen

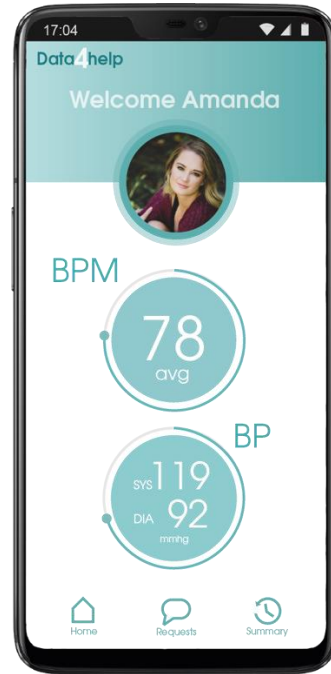


Figure 2 Mock up - Home screen

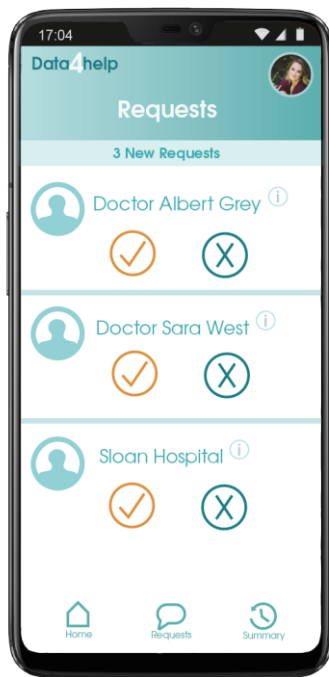


Figure 3 Mock up - Requests screen

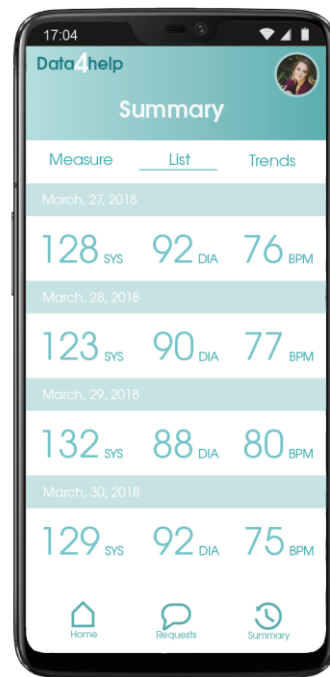


Figure 4 Mock up - Summary screen

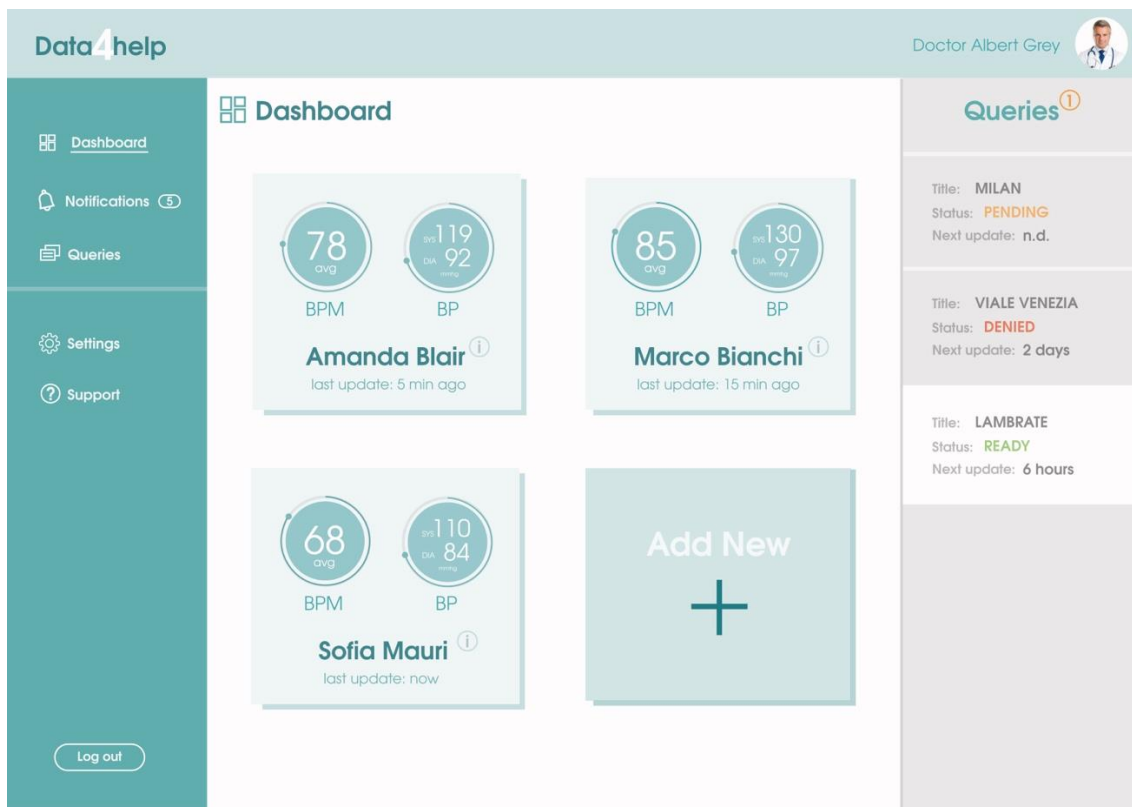



Figure 5 Mock Up – Dashboard Web App

Data4help

Doctor Albert Grey


Dashboard

Notifications 5

Queries

Settings

Support

Log out

Queries

Create a new query

Title:

Periodical update:
☒ 1 a day

Data req:

☐ Average BP
☐ Average MIN OF SPORT

☐ Average BPM
☐ Daily KCAL

☐ Average STEPS
☐ ...

Age:
From To

Time period:
From To

Location:

Within km:

Figure 6 Mock Up – Query Form

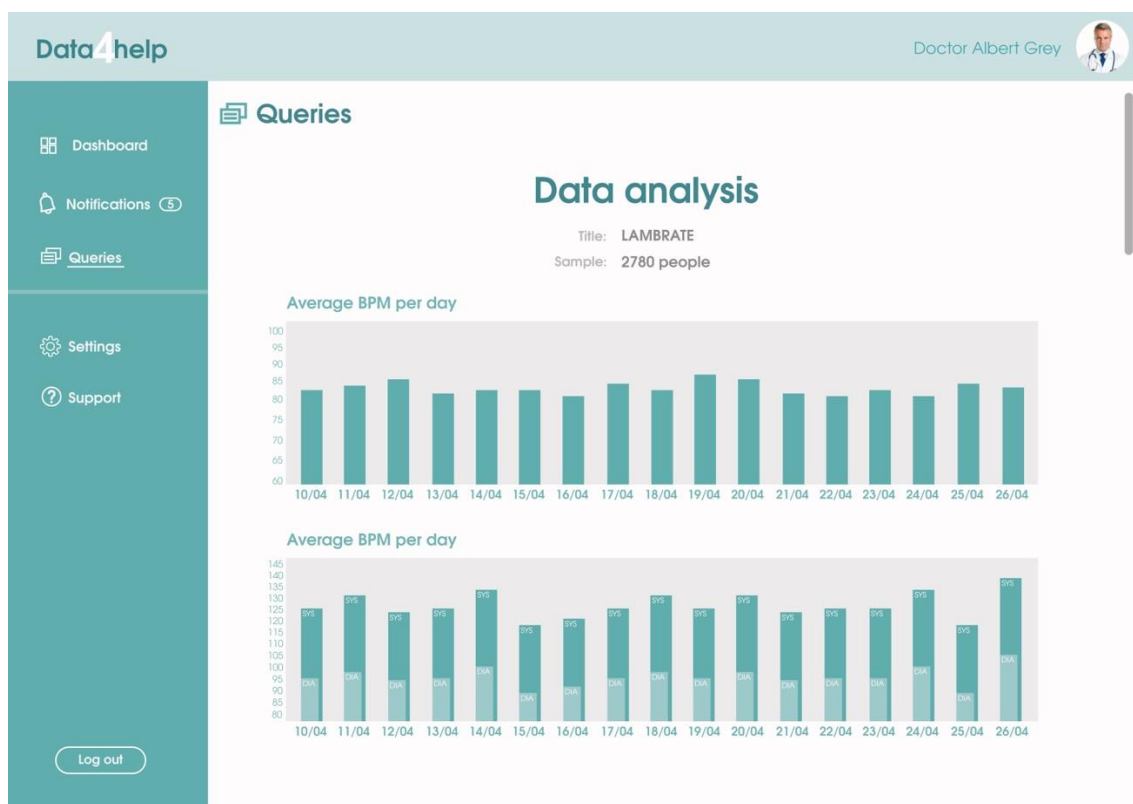


Figure 7 Mock Up – Query Result

3.1.2 Hardware Interfaces

Data4Help will not supply directly any hardware interface. To help Private Customers Data4Help will provide a list of compatible devices.

3.1.3 Software Interfaces

Data4Help will be developing:

- A smartphone application for the Private Customers to review their data and interact with the functionalities provided by the service.
- A web application for the Business Customers on which they are going to be able to submit queries, review Private Customers data and access all the functionalities of the service.

3.1.4 Communication Interfaces

Data4Help will provide a communication interface between the Private Customers subscribed to AutomatedSOS and the Emergency Room that will activate automatically when the PC's wearable detects an emergency.

3.2 FUNCTIONAL REQUIREMENTS

[G1] Allow a Visitor to become a Private Customer.

[D5] All information entered by the user during registration in the service is correct.

[R1] A Visitor must be able to register to the service by providing only the necessary requested personal information.

[R2] The system must ensure that the username chosen by the Visitor doesn't exist yet.

[R3] A registered user must be able to login using the credentials accepted during the registration process.

[R14] A visitor must accept the terms and conditions of the service.

[G2] Allow a Visitor to become a Business Customer.

[D5] All information entered by the user during registration in the service is correct.

[R2] The system must ensure that the username chosen by the Visitor doesn't exist yet.

[R3] A registered user must be able to login using the credentials accepted during the registration process.

[R15] A Visitor must be able to register to the service by providing only the necessary requested business' information.

[R14] A visitor must accept the terms and conditions of the service.

[R16] A visitor must provide correct billing information.

[G3] Allow a Private Customer to subscribe to AutomatedSOS.

[D4] There is an external service that will be in charge of the payment information validity and the secure payment transactions.

[R3] A registered user must be able to login using the credentials accepted during the registration process.

[G4] Allow a Private Customer to review personal data.

[D1] The device used by the user is able to provide accurate data on his/her health status.

[D2] The device used by the user is able to provide accurate data on his/her location.

[D8] The Wearable device is always paired with the Private Customer's phone

[D9] All the health information is always available through OS API's.

[R3] A registered user must be able to login using the credentials accepted during the registration process.

[R24] The system presents all the gathered data from the Private Customer.

[G5] Allow a Business Customer to monitor data from Data4Help.

[D1] The device used by the user is able to provide accurate data on his/her health status.

[D2] The device used by the user is able to provide accurate data on his/her location.

[D5] All information entered by the user during registration in the service is correct.

[D6] GPS signal and 4G signal must always be available.

[D8] The Wearable device is always paired with the Private Customer's phone

[D9] All the health information is always available through OS API's.

[R3] A registered user must be able to login using the credentials accepted during the registration process.

[R4] The system has to show to the BC all the available data (anonymized data or specific individual accepted data) with information on the date on which they were taken or the period they cover.

[R19] To monitor specific Private Customer's data, the request must be accepted by the PC.

[G6] Allow a Business Customer to request data from Data4Help.

[D5] All information entered by the user during registration in the service is correct.

[R3] A registered user must be able to login using the credentials accepted during the registration process.

[R5] The system has to show to the BC all the possible characteristics that the anonymized data to be requested can have.

[R6] The system has to show to the BC the two options he/she has: anonymized data or specific individual data.

[R7] The system will accept any request for which the number of individuals whose data satisfy the request is higher than 1000, if the number is lower, the request is rejected.

[G7] Allow a Private Customer to share his real time position and health status by a Business Customer.

[D5] All information entered by the user during registration in the service is correct.

[D8] The Wearable device is always paired with the Private Customer's phone

[D9] All the health information is always available through OS API's.

[R3] A registered user must be able to login using the credentials accepted during the registration process.

[R8] The system has to notify to the PC that a BC has requested to monitor his/her individual data.

[R9] The system has to show all the information about the BC that is requesting the permission.

[R10] The system gives the possibility to the PC to accept and refuse the request.

[G8] Allow a Business Customer to subscribe to a data source like a specific PC or a geographical area.

[D5] All information entered by the user during registration in the service is correct.

[R3] A registered user must be able to login using the credentials accepted during the registration process.

[R5] The system has to show to the BC all the possible characteristics that the anonymized data to be requested can have.

[R11] The system periodically updates the selected data.

[R12] The system updates the anonymized data only if guarantees on anonymity is respected, otherwise data are not updated.

[R20] The system notifies the BC each time subscribed data is changed.

[G9] Allow a PC in serious health conditions to receive an ambulance in the shortest possible time.

[D1] The device used by the user is able to provide accurate data on his/her health status.

[D2] The device used by the user is able to provide accurate data on his/her location.

[D3] The application has access to emergency numbers to call in case of emergency.

[D5] All information entered by the user during registration in the service is correct.

[D6] GPS signal and 4G signal must always be available.

[D8] The Wearable device is always paired with the Private Customer's phone

[D9] All the health information is always available through OS API's.

[R3] A registered user must be able to login using the credentials accepted during the registration process.

[R13] The mobile application has to be capable of making emergency calls through a vocal synthesizer.

[G10] Allow a System Manager to do operations of system maintenance.

[R21] The system manager must provide login credentials.

[G10.1] Allow a SM to verify and accept the request of appliance from a BC.

[D4] There is an external service that will be in charge of the payment information validity and the secure payment transactions.

[D5] All information entered by the user during registration in the service is correct.

[D7] A system manager is capable of find inconsistencies in the business' information.

[R22] The system must provide all the information about the subscription requests of the BC.

[R23] The system manager can approve a new BC.

3.3 NON-FUNCTIONAL REQUIREMENTS

3.3.1 Performance

The system of Data4Help needs to be able to handle multiple connection without any latency in order to collect in real time Private Customer's health data.

Business Customers will be able to:

- Inspect in real time the data acquired of a specific Private Customer.
- The result of the anonymized requests will be available in less than 24h. We assume that some queries might require significant time to be resolved due to their complexity that can lead to a queue rendering Data4Help unable to give real time results for the anonymous requests.

3.3.1.1 AutomatedSOS performance requirements

The system will also provide a 5 seconds response time from the detection of an emergency via the wearable Private Customer's device to the start of the call to the emergency phone line.

3.3.2 Reliability

The system needs to be online 24/7. Given its medical purpose TrackMe must opt to deploy a system of redundant servers, located in different places. This will in almost every case prevent any loss of data and any downtime.

3.3.2.1 AutomatedSOS reliability requirements

AutomatedSOS needs at least 10% of battery remaining on the smartphone in order to function reliably. It's assumed that this is required since in case of emergency the phone needs to stay active at least for another hour, to allow the Private Customer to communicate with the emergency room till the alleged arrival of the ambulance.

3.3.3 Security

The system needs to be secure both from the physical (Secure server room) and the digital perspective. This is critical in order to prevent any malicious loss or theft of data. In any circumstance the security of all data stored by Data4Help must be of the utmost priority.

The Client's data needs to be encrypted with AES.

All the connections through internet must be protected with TLS over HTTP.

3.3.4 Scalability

The system needs to be scalable as the userbase might increase over the initial design limit.

3.3.5 Accuracy

The hardware must provide accurate health data to render possible the implementation of AutomatedSOS functionality, lives will depend on this service.

GPS precision needs to be in the order of 10 meters to allow an effective rescue in case of emergency.

4 SCENARIOS

4.1 SCENARIO 1

Julia, unfortunately, has a rare disease. Due to this condition her health parameters need to be checked frequently by a medical equip. Thanks to Data4Help Julia can lead a normal life without worrying about going very often to a hospital. She is registered to Data4Help as a Private Customer and her equip as a Business Customer. Julia accepted the request from the medical equip to allow the real time monitoring function.

Now she can enjoy a normal life.

4.2 SCENARIO 2

Carlos works for a public hospital in Milan, he is an analyst and having precise health data of the people living in Milan can help him in his last research on air pollution. A colleague tells him that the hospital now is a Business Customer of Data4Help and informs him about the possibility of querying the Data4Help database to gather anonymous health data of the population of a certain area. Carlos is amazed by this information, the next day his superior will give him the credentials to use Data4Help service. After downloading Data4Help's desktop client software he can immediately start filling the "anonymous query" form. In the 24 hours succeeding the submission he will receive a notification on his desktop and the asked data will be available for consultation.

4.3 SCENARIO 3

Emilio has a very old mother. He always worries thinking that something may happen to her when she's alone. After an internet research he comes to know that Data4Help has recently opened to the public a service called AutomatedSOS that provides immediate rescue in case of swoon or hearth attack. He immediately thinks that this seems tailored to his needs. After talking with her mother, Emilio downloads the Data4Help app on her smartphone and buys her a smart watch capable of monitoring blood pressure and heart rate. He registers his mother to Data4Help on the app as a Private Customer and then purchase a subscription to AutomatedSOS. From now on he will sleep peacefully not worrying about his mother health condition.

4.4 SCENARIO 4

Anna is a doctor who is studying the health of children living in a specific area of Milan. She needs continuously updated data, so she registers to TrackMe's Data4Help service and subscribes to the information she needs for her analysis. Since the search is very specific, after a while, she gets a notification from TrackMe that warns her that her request no longer respects the parameters. To overcome this problem, Anna is forced to expand the search area, in order to have enough people and to allow TrackMe to guarantee security policies on the anonymity of data.

4.5 SCENARIO 5

Giovanni is a very old man and has been registered by his sons in TrackMe's AutomatedSOS service, so that his health can always be monitored and in case of an emergency he can be helped in the shortest possible time, without the need for an always present person with him. One day he is home alone and is struck by a sudden illness that causes him to plunge into very serious health condition. Immediately his heath parameters are analyzed by AutomatedSOS that, within 5 seconds, contact the emergency service to have an ambulance where Giovanni is.

Without AutomatedSOS Giovanni would not have had the necessary help in time.

4.6 SCENARIO 6

Tommaso, a TrackMe's system manager, must verify the information of a Business Customer who wants to subscribe to the Data4Help service. Tommaso logs in on the platform providing his credentials and displays all the information of the Business Customer. After a careful analysis of the information, he proceeds to forward the payment to the external service that deals with the transactions. Once the payment is accepted, Tommaso can complete the registration process and confirm the new Business Customer.

5 UML MODELLING

5.1 USE CASE DESCRIPTIONS

5.1.1 Visitor registration as a Private Customer

<i>Actors</i>	Visitor
<i>Goals</i>	[G1]
<i>Input Conditions</i>	The visitor has downloaded the application on his/her smartphone
<i>Event Flow</i>	<ol style="list-style-type: none">1. The visitor clicks the “sign in” button in on the app2. The visitor fills the forms with the required personal information such as: e-mail, password, name, surname, CF or SSC, age, sex and birth place and date.3. The system checks for duplicates and correctness of the data provided.4. The visitor clicks “Confirm and Accept the terms and conditions of use”5. The system saves the information and sends a verification email to his address.6. The visitors verify his e-mail by clicking on the link sent to his address.
<i>Output Conditions</i>	The visitor now is a new Private Customer and it can Login on to the application and start using Data4Help service
<i>Exceptions</i>	<ol style="list-style-type: none">1. The visitor provides some identifying information already present in the system. (e-mail or CF or SSC)2. The visitor provides inconsistent data such as not matching CF to personal data. <p>These exceptions are handled by notifying the visitor the specific issue and presenting again a form to fill.</p>

5.1.2 Visitor registration as a Business Customer

<i>Actors</i>	Visitor
<i>Goals</i>	[G2]
<i>Input Conditions</i>	The visitor is on the web page of Data4Help
<i>Event Flow</i>	<ol style="list-style-type: none">1. The visitor clicks on “Register as a Business Customer” button on the main web page of Data4Help.2. The visitor provides all the information regarding his/her business, e-mail and password.3. The system checks for duplicates and inconsistencies in the provided data.4. The visitor clicks on “Confirm and Accept the terms and conditions of use”.5. The visitors verify his/her e-mail by clicking on the link sent to his/her address.
<i>Output Conditions</i>	The visitor now is a potential new Business Customer, awaiting confirmation from the System Manager
<i>Exceptions</i>	<ol style="list-style-type: none">1. The visitor provides some identifying information already present in the system. (e-mail, EIN or p.IVA). <p>These exceptions are handled by notifying the visitor the specific issue and presenting again a form to fill.</p>

5.1.3 Accepting Business Customer's requests of subscription to Data4Help

<i>Actors</i>	System Manager
<i>Goals</i>	[G10.1]
<i>Input Conditions</i>	The System Manager must be logged in to the maintenance system.
<i>Event Flow</i>	<ol style="list-style-type: none">1. The SM selects a request to process on the list presented on the main page of the maintenance system.2. The SM does a manual check on the information provided by the Business Customer3. The SM confirms the information.4. The system requests a payment through a third-party billing service.5. The payment is accepted.6. The SM updates system's information about subscribed Business Customers.
<i>Output Conditions</i>	The Business Customer is now a subscriber of Data4Help, allowing it to access all the functionalities offered by the platform.
<i>Exceptions</i>	<ol style="list-style-type: none">1. The system manager finds an inconsistency in the information provided2. The payment doesn't go through <p>In these exceptions the System Manager must manually contact the Business Customer to resolve the issues.</p>

5.1.4 Private Customer's subscription to AutomatedSOS

<i>Actors</i>	Private Customer
<i>Goals</i>	[G3]
<i>Input Conditions</i>	The Private Customer has already logged in to the Data4Help's application.
<i>Event Flow</i>	<ol style="list-style-type: none"> 1. The visitor clicks the "AutomatedSOS" button in on the app 2. The PC chooses the payment method that he/she wants to use, provided by a third-party billing service. 3. The PC is redirected to the chosen billing service page 4. The PC returns to the app that confirms that the payment has been entered successfully. 5. The PC receives an email that summarizes the operation and confirms the successful registration to the AutomatedSOS service.
<i>Output Conditions</i>	The Private Customer is now a subscriber of AutomatedSOS.
<i>Exceptions</i>	<ol style="list-style-type: none"> 1. Problems when entering payment information. <p>The PC returns to the app that tells him/her the process was not successful. He/she can try again or contact customer support.</p>

5.1.5 Business Customer's request of anonymized data

<i>Actors</i>	Business Customer
<i>Goals</i>	[G6] [G6.2]
<i>Input Conditions</i>	The Business Customer has already logged in to the Data4Help's web application.
<i>Event Flow</i>	<ol style="list-style-type: none"> 1. The BC goes in the section where to query for anonymized data. 2. The BC select a request of anonymized data. 3. The BC selects all the various parameters necessary to filter the people considered. 4. The BC confirms to proceed with the request.
<i>Output Conditions</i>	The BC can see the data he/she had requested
<i>Exceptions</i>	<ol style="list-style-type: none"> 1. The number of individuals whose data satisfy the request is lower than 1000. <p>The BC is notified to the system, which informs him/her that it cannot proceed with this type of request.</p>

5.1.6 Business Customer's request of specific individual data

<i>Actors</i>	Business Customer
<i>Goals</i>	[G6] [G6.1]
<i>Input Conditions</i>	The Business Customer has already logged in to the Data4Help's web application.
<i>Event Flow</i>	<ol style="list-style-type: none"> 1. The BC goes in the section where to query for anonymized data. 2. The BC select a request of specific individual data. 3. The BC inserts the SSN or the CF of the user he/she wants to monitor. 4. The BC confirms to proceed with the request.
<i>Output Conditions</i>	The BC is now waiting for the PC to accept his request. Then it will be able to see the requested data.
<i>Exceptions</i>	<ol style="list-style-type: none"> 1. No individual associated with that specific SSN or CF exists in the database The BC is notified to the system, which informs him/her that it cannot proceed with this type of request. 2. The SSN or the CF inserted are inconsistent. A notification informs the BC to change this field to make it consistent.

5.1.7 Business Customer's subscription to a specific data

<i>Actors</i>	Business Customer
<i>Goals</i>	[G8]
<i>Input Conditions</i>	The Business Customer has already logged in to the Data4Help's web application.
<i>Event Flow</i>	<ol style="list-style-type: none"> 1. The BC goes in the section where to make a subscription to a specific data. 2. The BC fills all fields providing the information necessary to proceed with the request. 3. The BC confirms to proceed with the request.
<i>Output Conditions</i>	The BC can now see the data he/she had requested
<i>Exceptions</i>	<ol style="list-style-type: none"> 1. No individual associated with that specific SSN or CF exists in the database (in case of specific individual to monitor) 2. The number of individuals whose data satisfy the request is lower than 1000 (in case of anonymized data) The BC is notified to the system, which informs him/her that it cannot proceed with this type of request.

5.1.8 Business Customer's monitor of requested data

<i>Actors</i>	Business Customer
<i>Goals</i>	[G5] [G5.1] [G5.2]
<i>Input Conditions</i>	The Business Customer has already logged in to the Data4Help's web application.
<i>Event Flow</i>	<ol style="list-style-type: none"> 1. The BC goes in his/her personal section of requested data accepted. 2. The BC search for the right data. 3. The BC selects the data he/she wants to monitor.
<i>Output Conditions</i>	The BC sees the data he/she had requested
<i>Exceptions</i>	<ol style="list-style-type: none"> 1. No data is available for the BC. The system notifies to the user that there aren't data to show.

5.1.9 Private Customer accepts the request from a Business Customer

<i>Actors</i>	Private Customer
<i>Goals</i>	[G7]
<i>Input Conditions</i>	The Private Customer has already logged in to the Data4Help's application.
<i>Event Flow</i>	<ol style="list-style-type: none"> 1. The PC goes in the section "Incoming request" 2. The PC chooses the request he/she has to accept/refuse. 3. The PC sees all the information about the BC is requesting the permission to monitor the data. 4. The PC click on "Accept".
<i>Output Conditions</i>	The BC now can monitor the PC that has accepted his/her request.
<i>Exceptions</i>	//

5.1.10 Private Customer reviews personal data.

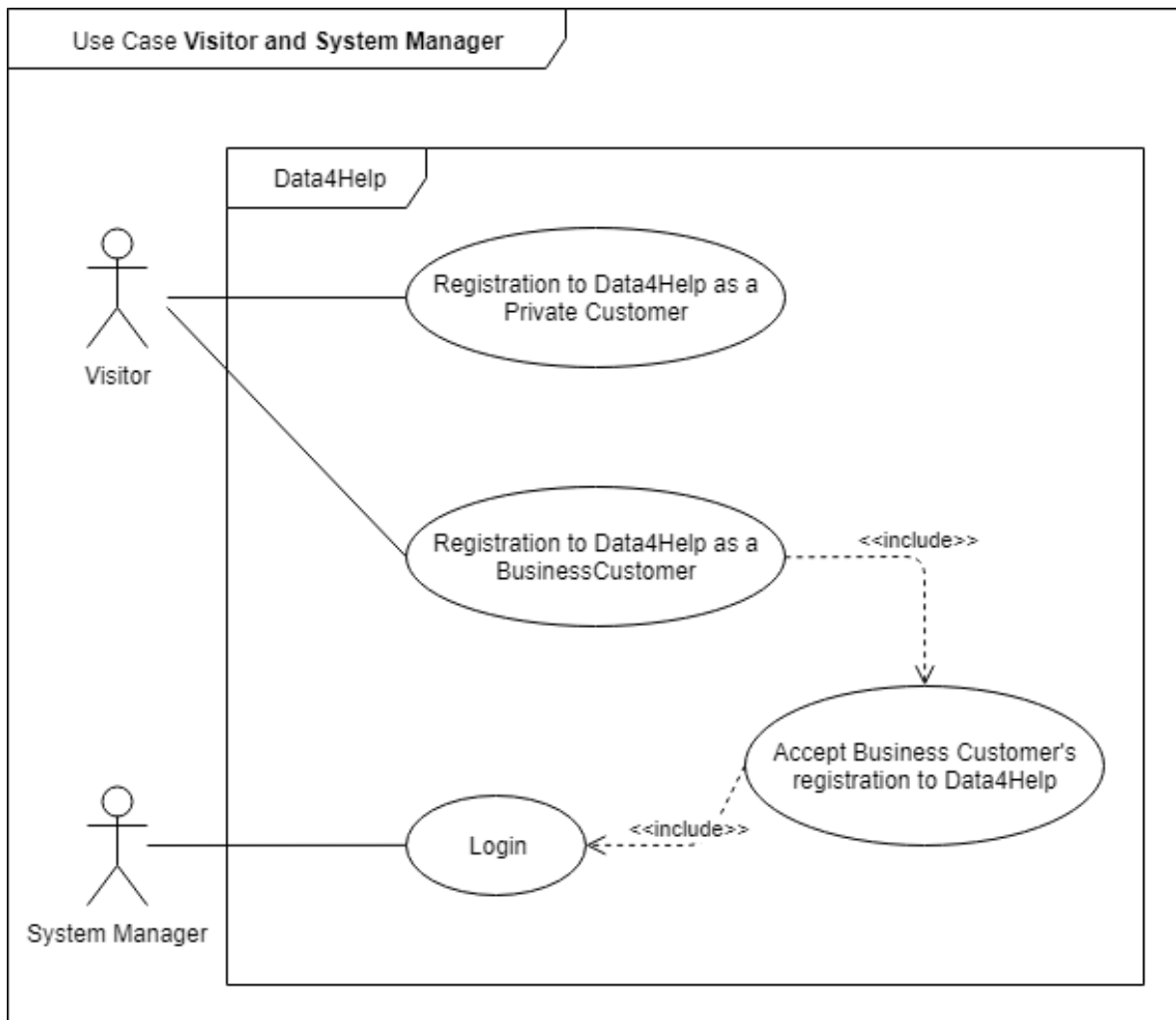
<i>Actors</i>	Private Customer
<i>Goals</i>	[G4]
<i>Input Conditions</i>	The Private Customer has already logged in to the Data4Help's application.
<i>Event Flow</i>	1. The PC goes in the section "Personal Data" 2. The PC selects a time period 3. The system presents all the requested data.
<i>Output Conditions</i>	The PC can now review his personal data.
<i>Exceptions</i>	There is no personal data. The user is notified whit a message.

5.1.11 AutomatedSOS: Emergency

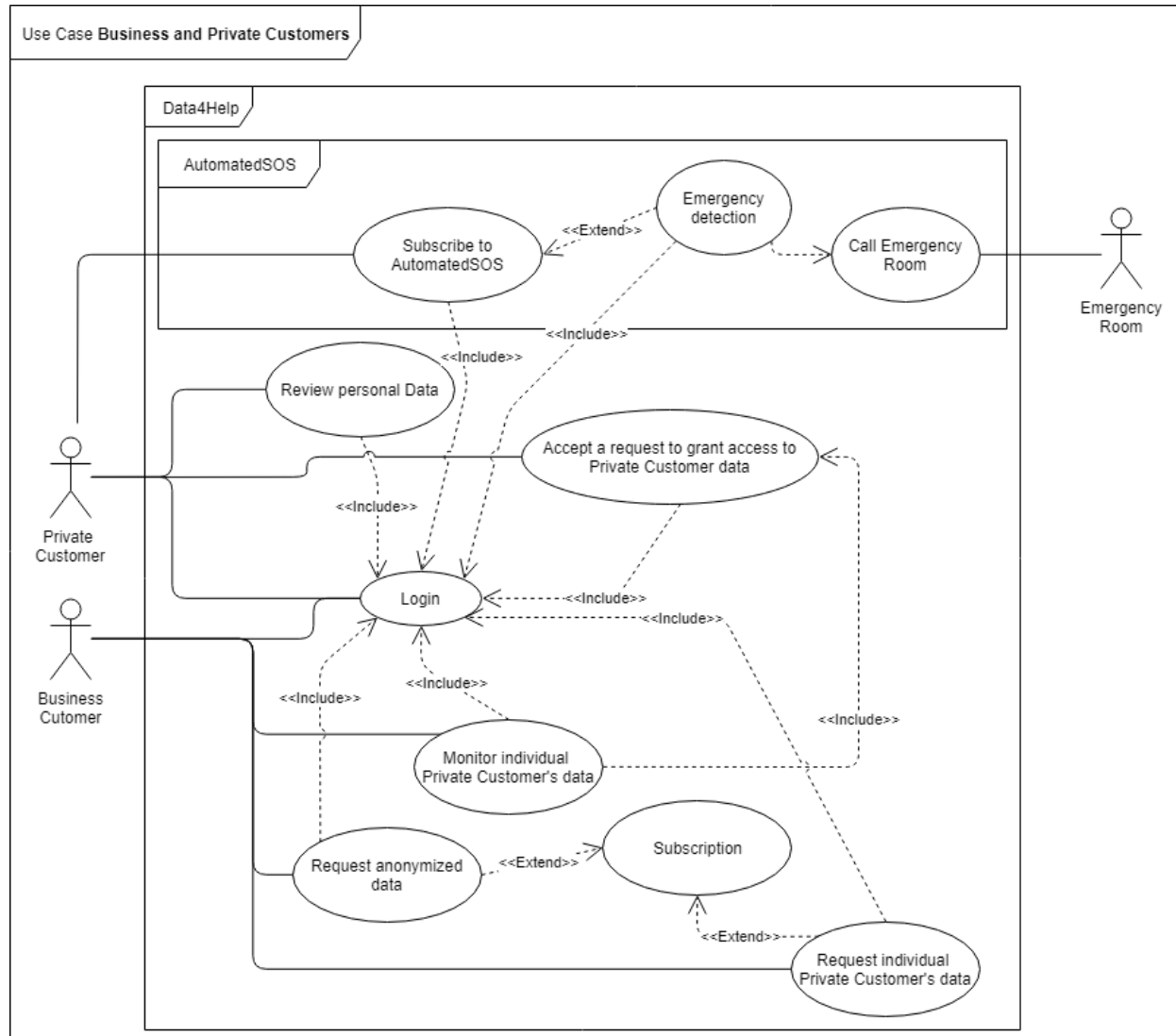
<i>Actors</i>	Private Customer
<i>Goals</i>	[G9]
<i>Input Conditions</i>	The Private Customer has already logged in to the Data4Help's application and one or more of his health parameters are below threshold
<i>Event Flow</i>	//
<i>Output Conditions</i>	The Private Customer will be put in contact with the nearest Emergency Room.
<i>Exceptions</i>	No exceptions are contemplated in this use case.

5.2 USE CASE DIAGRAMS

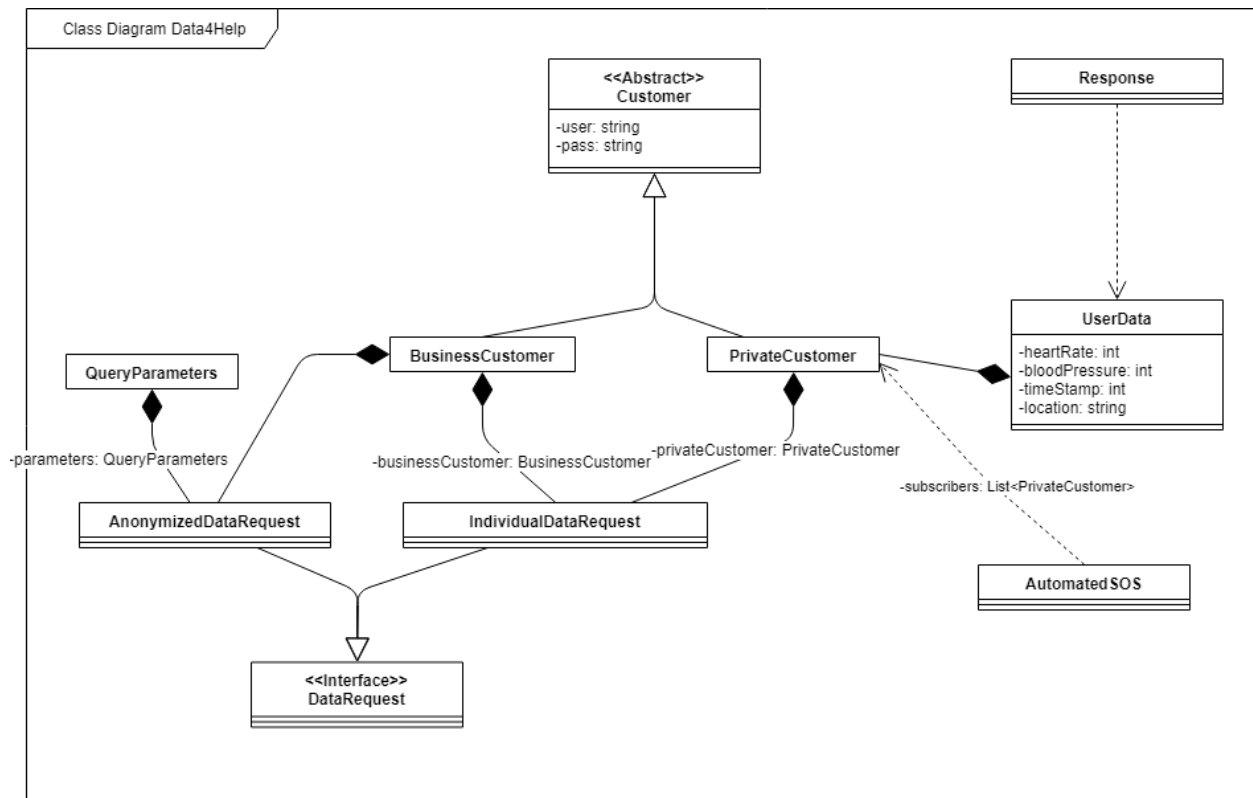
5.2.1 Use case visitor and system manager



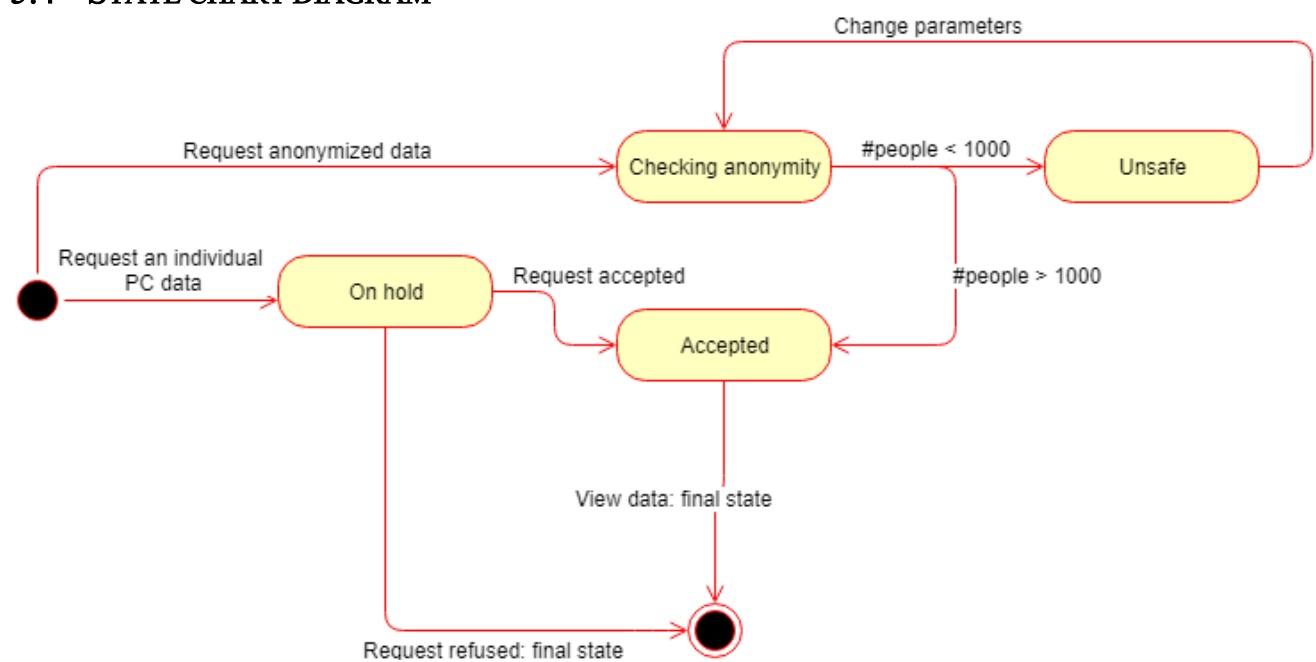
5.2.2 Use case Business and Private customers



5.3 CLASS DIAGRAM

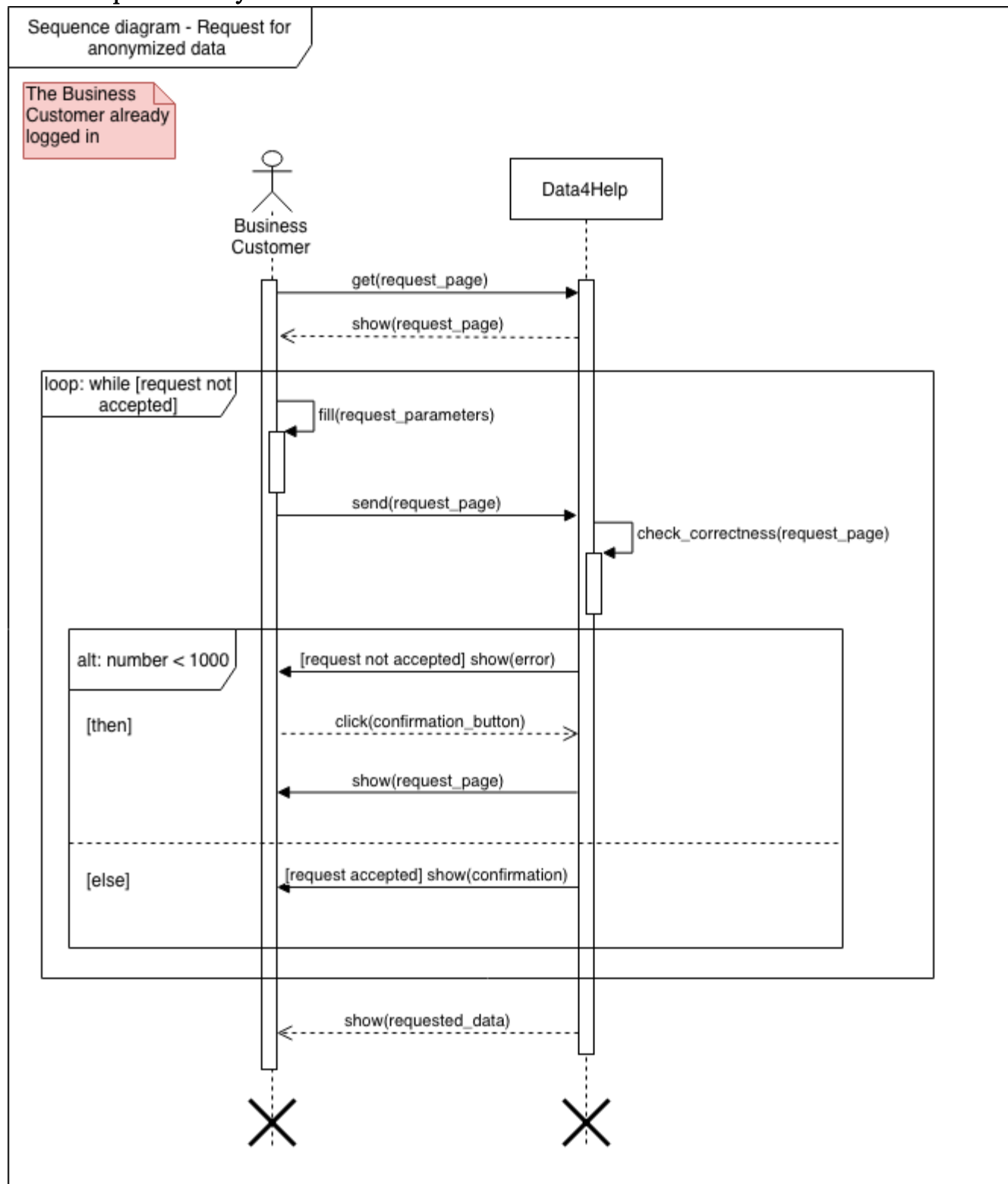


5.4 STATE CHART DIAGRAM

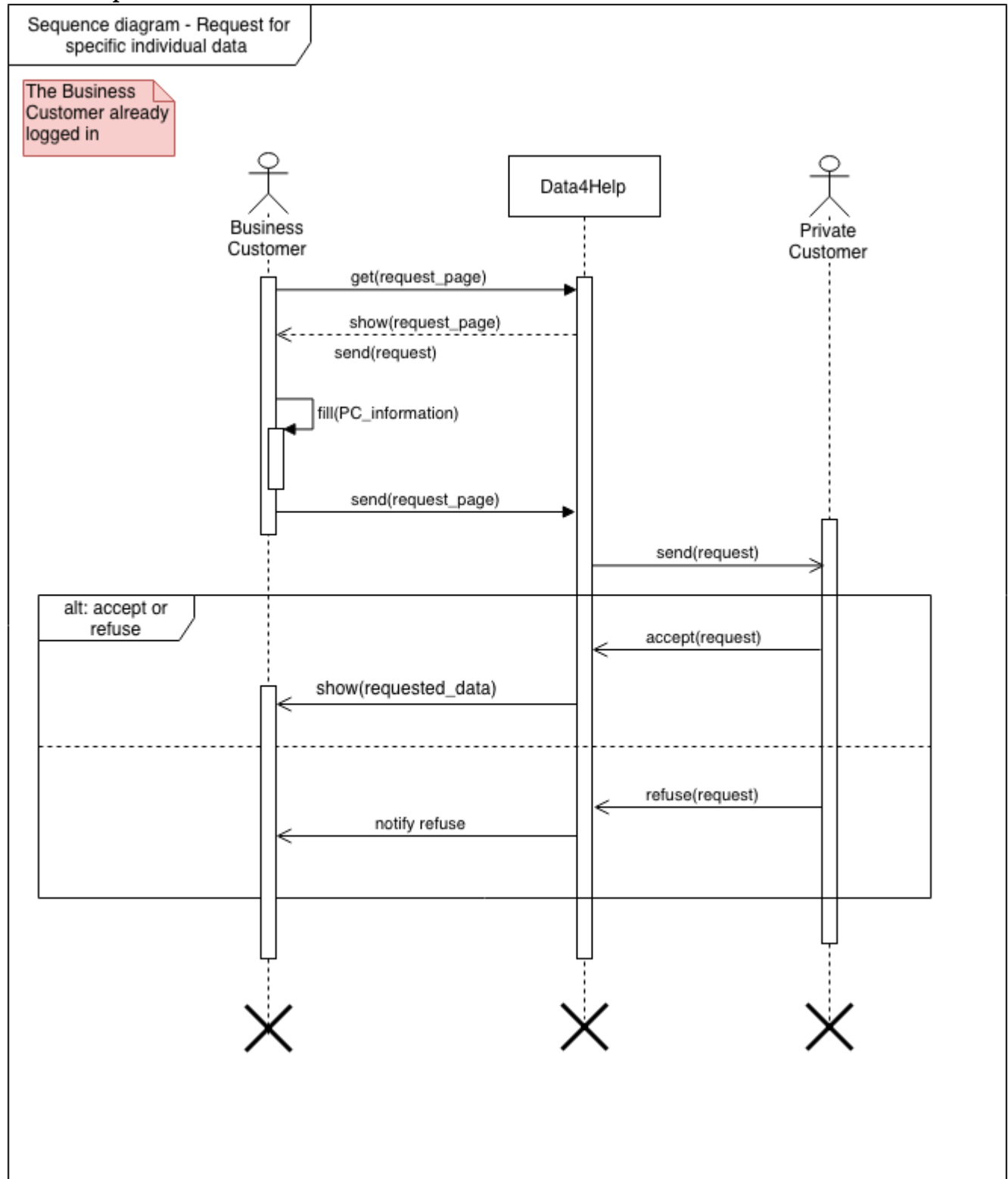


5.5 SEQUENCE DIAGRAM

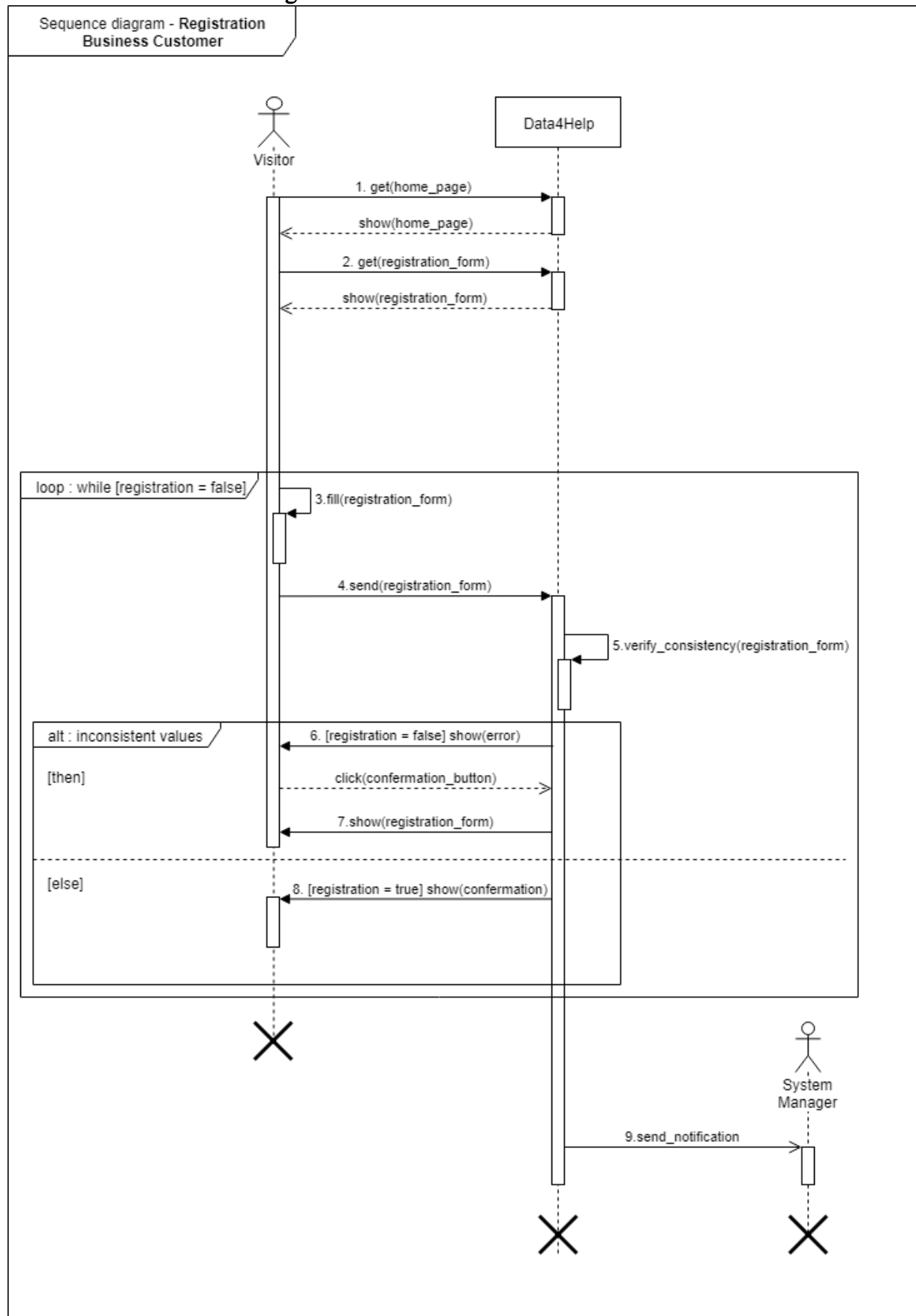
5.5.1 Request of anonymized data



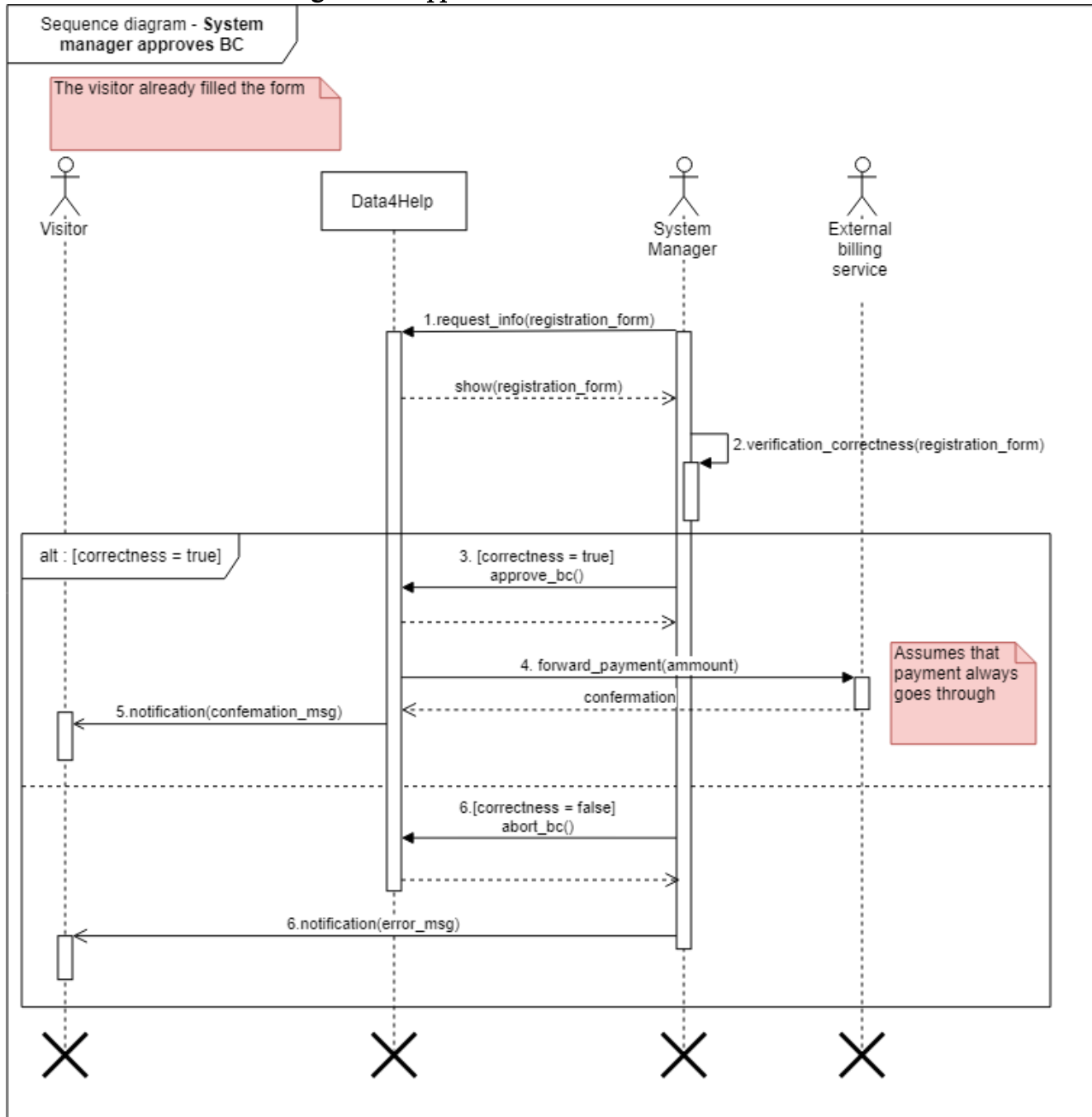
5.5.2 Request for individual data



5.5.3 Business Customer registration



5.5.4 Business Customer registration approval



6 Formal analysis using Alloy

```
open util/integer
open util/boolean
open util/time
open util/ordering [Time]

abstract sig HealthStatus{}
one sig HealthyConditions extends HealthStatus{}
one sig SeriousConditions extends HealthStatus{}

abstract sig RequestStatus{}
one sig AcceptedStatus extends RequestStatus{}
one sig DeniedStatus extends RequestStatus{}

sig Location{}

sig UserData{
  heartRate: one Int,
  bloodPressure: one Int,
  timeStamp: one Int,
  location: one Location
}

sig Username{}

--Service that deals with sending notifications when new data is available
one sig Notification{
  notifications: BusinessCustomer set -> Time
}

abstract sig Customer{
  username: one Username
}
```

Signatures 1

```
sig PrivateCustomer extends Customer{
  automatedSOS: one Bool,
  emergencyCall: one Bool,
  status: one HealthStatus,
  personalData: one UserData, --realtime data
  recordData: set UserData, --past data
  requests: IndividualRequest set -> Time
}

--the dimension of the requests can only increasing
all t1:Time | no t2:Time | t2 in t1.nexts and #requests.t2 < #requests.t1

--personalData is always the most recent data
max[recordData.timeStamp] < personalData.timeStamp
}

sig BusinessCustomer extends Customer{
  anonRequests: AnonymizedRequest set -> Time,
}

abstract sig Request{
  subscription: one Bool,
  newDataAvailable: Bool one -> Time,
  bc: one BusinessCustomer
}

sig IndividualRequest extends Request{
  status: RequestStatus one -> Time
}

--At the beginning each individual request is denied, because it has not been accepted yet
one t:Time | t = min[Time] and status.t = DeniedStatus
}
```

Signatures 2

```

sig AnonymizedRequest extends Request{
  numberOfPeople: some PrivateCustomer
}

one sig AutomatedSOS{
  subscribed: set PrivateCustomer,
  emergencyCall: set PrivateCustomer -> Bool
}

```

Signatures 3

```

fact customerRules{
  --All usernames must be different
  no disj c1,c2: Customer | c1.username = c2.username

  --All userData belongs to only one customer
  all disj pc1,pc2: PrivateCustomer | no data: UserData |
    (data in pc1.recordData and data in pc2.recordData) or
    (data in pc1.personalData and data in pc2.recordData) or
    (data in pc1.personalData and data in pc2.personalData) or
    (data in pc1.recordData and data in pc2.personalData)

  --For each userData exist one PrivateCustomer in which userData is contained
  all data: UserData | one pc: PrivateCustomer | data in pc.recordData or data in pc.personalData
}

fact requestRules{
  -- No individual request linked to two different private customers should exist
  all disj pc1,pc2: PrivateCustomer, t:Time | no r: IndividualRequest | r in pc1.requests.t and r in pc2.requests.t

  --All accepted request must be linked with a private customer
  all i:IndividualRequest , t: Time | i.status.t = AcceptedStatus iff one pc: PrivateCustomer | i in pc.requests.t

  --All requests belong to the same privateCustomer, at all the following times
  all r: IndividualRequest, t: Time | all pc: PrivateCustomer | r in pc.requests.t implies
    (all t2: Time | t2 in t.nexts implies (r in pc.requests.t2))

  --All anonymized requests belong to the same BusinessCustomer
  all a: AnonymizedRequest, t: Time | all bc: BusinessCustomer | a in bc.anonRequests.t implies
    (all t2: Time | t2 in t.nexts implies (a in bc.anonRequests.t2))
}

fact emergencySituation{
  all pc: PrivateCustomer | pc.status = SeriousConditions iff
    (pc.personalData.heartRate > 130 or pc.personalData.heartRate < 50
    or pc.personalData.bloodPressure > 130 or pc.personalData.bloodPressure < 60)
}

```

Facts 1

```

fact noEmergencyCallForUnsubscribed{
  --AutomatedSOS service is valid only for those subscribed Private Customer
  all pc: PrivateCustomer | pc in AutomatedSOS.subscribed iff pc.automatedSOS = True
}

fact emergencyCall{
  --Emergency call is done only if a subscribed PC is in serious conditions
  all pc: PrivateCustomer | pc.emergencyCall = True iff
    (pc in AutomatedSOS.subscribed and pc.status = SeriousConditions)
}

fact notificationOfUpdate{
  --There may be new anonymized data only if a subscription has been requested
  all r: AnonymizedRequest, t: Time | r.newDataAvailable.t = True implies r.subscription = True

  --There may be new individual data only if a subscription has been requested and the request has been accepted
  all r: IndividualRequest, t: Time | r.newDataAvailable.t = True implies (r.subscription = True and r.status.t = AcceptedStatus)

  --If there is new available data a notification must be sent
  all r: Request, t: Time | no bc1: BusinessCustomer | bc1 = r.bc
    and r.newDataAvailable.t = True and bc1 not in Notification.notifications.t

  --Only the BCs who have requests with new available data can be notified
  all t: Time | no bc1: BusinessCustomer |
    bc1 in Notification.notifications.t and no r: Request | bc1 = r.bc and r.newDataAvailable.t = True
}

```

Facts 2

```

pred makeIndividualRequest[i: IndividualRequest, t1, t2: Time, pc, pc': PrivateCustomer]{
  // precondition
  not i in pc.requests.t1
  // postconditions
  t2 = t1.next
  pc'.requests = pc.requests + i -> t2
}

pred makeAnonymizedRequest[a: AnonymizedRequest, t1, t2: Time, bc, bc': BusinessCustomer]{
  //precondition
  not a in bc.anonRequests.t1

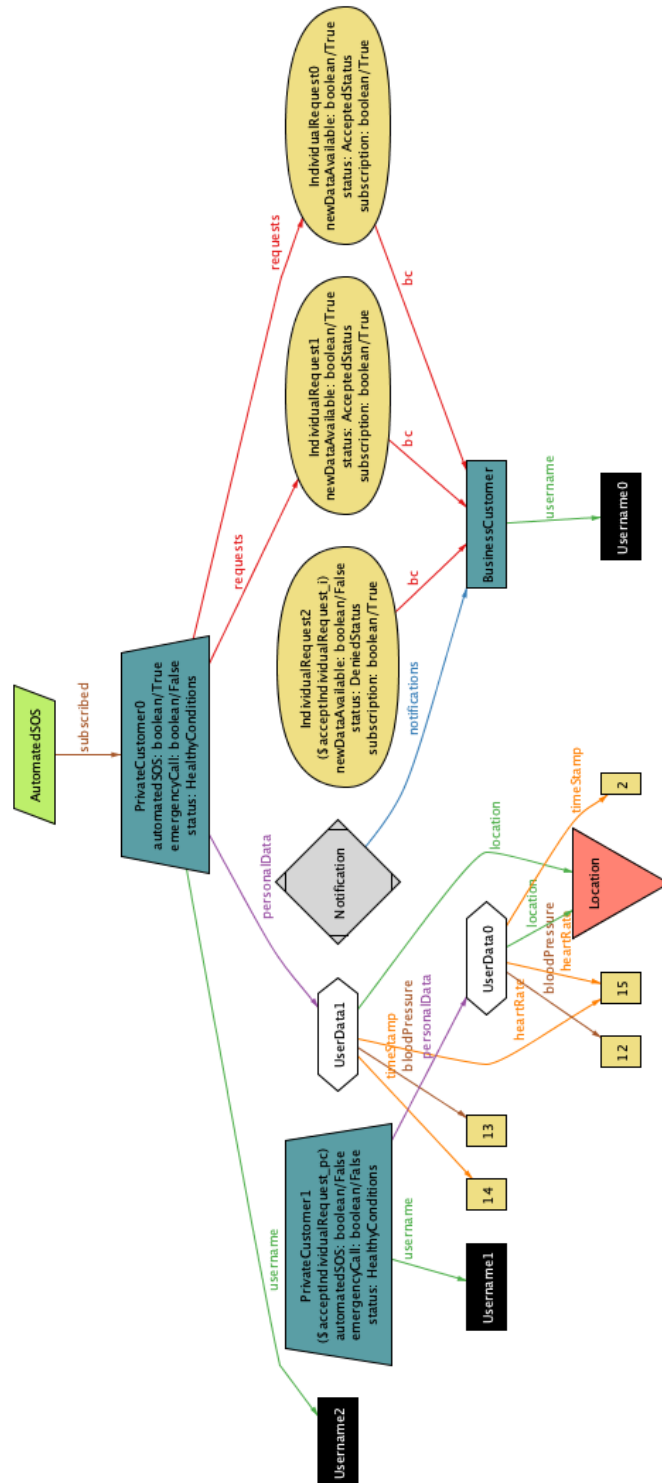
  //postconditions
  t2 = t1.next
  bc'.anonRequests = bc.anonRequests + a -> t2
}

pred acceptIndividualRequest[i : IndividualRequest, t1, t2: Time,pc:PrivateCustomer]{
  //precondition
  i in pc.requests.t1

  //postconditions
  i.status.t1 = DeniedStatus implies i.status.t2 = AcceptedStatus
  t2 = t1.next
}

```

Predicates 1



Sample of world generated 1

[illegible]

6.1 ALLOY RESULTS

run makeAnonymizedRequest for 7 but 8 Int, exactly 1 AnonymizedRequest, exactly 1 IndividualRequest
run makeIndividualRequest for 10 but 8 Int, exactly 1 IndividualRequest, exactly 6 UserData, exactly 6 PrivateCustomer
run acceptIndividualRequest for 5 but 5 Int, exactly 3 IndividualRequest, exactly 2 PrivateCustomer

Run Commands

Executing "Run makeIndividualRequest for 10 but 8 int, exactly 1 IndividualRequest, exactly 6 UserData, exactly 6 PrivateCustomer"
Solver=sat4j Bitwidth=8 MaxSeq=10 SkolemDepth=1 Symmetry=20
183754 vars. 5754 primary vars. 839313 clauses. 831ms.
Instance found. Predicate is consistent. 4491ms.

Result 1

Executing "Run makeAnonymizedRequest for 7 but 8 int, exactly 1 AnonymizedRequest, exactly 1 IndividualRequest"
Solver=sat4j Bitwidth=8 MaxSeq=7 SkolemDepth=1 Symmetry=20
212234 vars. 5913 primary vars. 996276 clauses. 1232ms.
Instance found. Predicate is consistent. 3177ms.

Result 2

Executing "Run acceptIndividualRequest for 5 but 5 int, exactly 3 IndividualRequest, exactly 2 PrivateCustomer"
Solver=sat4j Bitwidth=5 MaxSeq=5 SkolemDepth=1 Symmetry=20
10076 vars. 787 primary vars. 18751 clauses. 53ms.
Instance found. Predicate is consistent. 66ms.

Result 3

7 EFFORT SPENT

Task	<i>Tommaso Peresson</i>	<i>Giacomo Ziffer</i>
Specifications and goals	4	4
Goals and assumptions	4	4
Requirements	6	6
Diagrams	3	3
Alloy	8	10
Various	5	5
TOTAL	30	32