



POLITECNICO
MILANO 1863

Politecnico di Milano

AA 2018-2019

Computer Science and Engineering
Software Engineering 2 Project

Dalle Rive Fabio - 920082

Di Giacomantonio Marco - 846515

Table of Contents

1. Introduction
 - 1.1. Purpose
 - 1.2. Scope
 - 1.2.1.. Description of the given problem
 - 1.2.2.. Goals
 - 1.3. Definitions, Acronyms, Abbreviations
 - 1.3.1.. Definitions
 - 1.3.2.. Acronyms
 - 1.3.3.. Abbreviations
 - 1.4. Document structure
2. Overall Description
 - 2.1. Product perspective
 - 2.2. Product functions
 - 2.2.1..
 - 2.3. User characteristics
 - 2.4. Assumptions, dependencies and constraints
 - 2.4.1.. Domain assumptions
3. Specific requirements
 - 3.1. External interface requirements
 - 3.1.1.. Users interfaces
 - 3.1.2.. Hardware interfaces
 - 3.1.3.. Software interfaces
 - 3.1.4.. Communication interfaces
 - 3.2. Scenarios
 - 3.2.1..
 - 3.3. Functional requirements
 - 3.3.1.. Use case diagram
 - 3.3.2.. Sequence diagram
 - 3.4. Performance requirements
 - 3.5. Design Constraints
 - 3.5.1.. Standard compliance
 - 3.5.2.. Hardware limitation
 - 3.5.3.. Other constraint

- 3.6. Software system attributes
 - 3.6.1.. Reliability
 - 3.6.2.. Security
 - 3.6.3.. Maintainability
 - 3.6.4.. Compatibility
- 4. Formal Analysis Using Alloy
 - 4.1. Alloy model
 - 4.2. World generated
 - 4.3. Alloy results
- 5. Effort Spent
- 6. Resources

1 Introduction

1.1 Purpose

The purpose of this project is to build a system, called Data4Help, that allows third parties to monitor the position and health status of users. The data are collected by TrackMe, the company that wants to develop Data4Help, and are shared with other companies which are interested in those data. Furthermore, TrackMe wants to develop AutomatedSOS, a system build on top of Data4Help. AutomatedSOS is a service designed for elderly people, it is able to intervene by calling an ambulance if the health parameters of the user are below some fixed thresholds.

1.2 Scope

1.2.1 Description of the given problem

TrackMe is a company that wants to develop a software-based service allowing third parties to monitor the location and health status of users. This service is called Data4Help. The service supports the registration of the visitors who, by registering, allow TrackMe to acquire their data. Also it supports the registration of third parties. After registration, these third parties can request:

- Access to the data of some specific user.
- Access to anonymized data of groups of users.

TrackMe also wants to develop a non-intrusive SOS service for elderly people, called AutomatedSOS. AutomatedSOS is build on top of Data4Help. This service is designed to monitor health status of users and to send an ambulance to the location of the user if some parameters are below some specified thresholds.

1.2.2 Goals

- [G1] Visitor can become User after providing credentials.
- [G2] User can accept or reject the request of access to his data formulated by companies.
- [G3] If user's parameters are below specified thresholds, an ambulance is called within 5 seconds.
 - [G3.1] Ambulance is required at current user's location.
- [G4] Company can sign up as Company to Data4Help and AutomatedSOS.
- [G5] Company can be recognized providing a password and vat number.
- [G6] Company can formulate a request to see anonymized data of a group of users.

- [G7] Company can formulate a request to see data of a specific user providing his SSN.
- [G8] Company can see anonymized data of a group of users.
- [G9] Company can see data of a specific user providing his SSN.
- [G10] Company can subscribe to users' new data.
- [G11] Data4Help can anonymise data.
- [G12] Data4Help can forward companies' requests to users.
- [G13] ??? TrackMe able to withdraw a company ????

1.3 Definitions, Acronyms, Abbreviations

1.3.1 Definitions

- **Visitor:** a person who still has to register to Data4Help and AutomatedSOS.
- **User:** a person who is registered to Data4Help and AutomatedSOS.
- **Third Parties / Companies:** company.
- **Data:** User's monitored data: location + heart rate + calories burned + time spent exercising + step walked
- **Threshold:** Flexible value related to the biomedical data acquired by the smart watch in which the system-to-be is installed. This value is computed by well-known equation that operate with user's data. It also depends of the kind of activity that a user is doing.
- **Request:** Formal request that a company issue to Data4Help in order to access data of a single user or a group of users.
- **Subscribe to data:** A company which is subscribed to user's data or to users group's data, receives the requested data as soon as they are produced.
- **Pendent user:** A user that a company want to follow but has not answered to the following request yet.
- **Single user request / Following request:** A formal request issued by a company to see the data of a user.
- **Group of users request:** A formal request issued by a company to see the data of a group of users.

1.3.2 Acronyms

- RASD - Required Analysis and Specification Document
- GPS - Global Positioning System
- SSN - Social Security Number

1.3.3 Abbreviations

- [Gn]: n-th goal
- [Dn]: n-th domain assumption
- [Rn]: n-th functional requirement

1.4 Document structure

Introduction gives an introduction to the problem and describe the purpose of Data4Help and AutomatedSOS. It also contains the goals that these systems-to-be must be able to deliver to users and third party companies.

Overall Description gives an overview of the functions that the systems-to-be are able to deliver to users and third parties. In this section, users of the systems-to-be, are better identified, i.e. the kind of users that interact with Data4Help and AutomatedSOS. Due to the imprecise nature of natural language used in the specification of the project, a more formal presentation of the assumptions is required. Assumptions used by Data4Help and AutomatedSOS are presented in this section.

Specific Requirements

Formal Analysis Using Alloy includes the Alloy model and the discussion of its purpose. Also, a world generated by this model is shown.

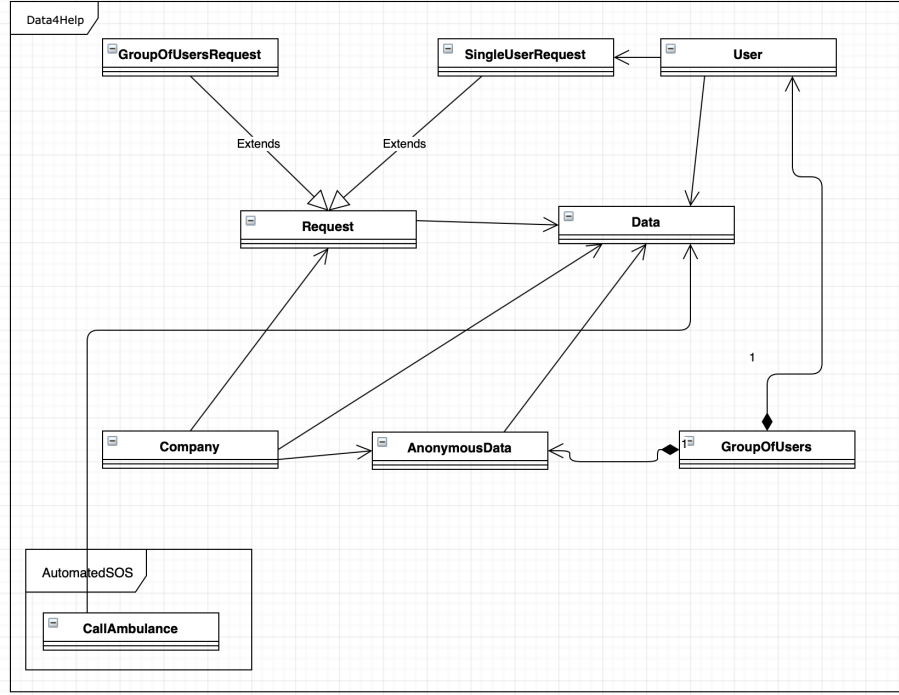
Effort Spent shows the effort spent by each group member while working on this project.

Resources includes the reference documents.

2 Overall Description

2.1 Product perspective

Data4Help and AutomatedSOS are intended as a background application that are installed inside a smart watch. The systems-to-be acquire data of the users through the smart watch. The user register himself for Data4Help on the website page that TrackMe provide for this application. Users access to the web page through their Google or Apple account. These accounts are used by TrackMe in order to understand from which devices it will acquire data.



2.2 Product functions

Considering all the goals previously presented, we can sum up into four categories the main functions of the product:

2.2.1 Acquisition of users' data

Data4Help runs on a smartwatch, assumed to be able to communicate the data directly to TrackMe's servers. It means that this product works only with smartwatch with an internet connection. Future updates will enable to use also smartwatch without internet connection to run Data4Help and AutomatedSOS.

2.2.2 Company access to users' data

Data4Help enables companies to access data of a specific user or of groups of users. Companies access to these data through the web page. Data are shown in a user-friendly way, generating automatically graphs. Some samples of the GUI will be shown in the corresponding section.

2.2.3 Forwarding of following requests directly to the users and data anonymization

Companies are able to send following requests, in order to access user data. Data4Help allows TrackMe to put in contact companies and users. Every time that a company request to access some data, Data4Help notifies TrackMe's servers. Analyzing the request, TrackMe's servers will decide how to proceed:

- If the request concerns a specific user, TrackMe sends an email to the user asking to accept or reject it
- If the request concerns a group of users, anonymizes the corresponding data

2.2.4 AutomatedSOS

While registering Data4Help, the user is asked to submit his age. Basing on some criteria chosen from the management, a value *Age* is chosen. If the user's age is greater than *Age* AutomatedSOS is activated automatically. AutomatedSOS is a service that monitors the heartbeat of the user and if it's lower than *Threshold*, calls an ambulance addressed to the user's position within 5 seconds.

2.3 User characteristics

- *Visitor*: a person not registered. The only thing he can do is proceeding with sign up.
- *User*: a person passed through a successful registration process. His data can be tracked, he can accept or reject companies' following request.
- *Company*: an entity that can be recognised as a company. It can see data of a specific user or anonymous data of a group of users.
- *TrackMe*: the whole hardware and software interfaces over which Data4Help and AutomatedSOS.

2.4 Assumption, dependencies and constraints

2.4.1 Domain assumptions

- [D1] The user's email is already known by TrackMe.
- [D2] Only real companies can sign up as companies.
- [D3] Only companies can see users' data.
- [D4] 5 seconds are necessary to send user location and call an ambulance when parameters are below the threshold.

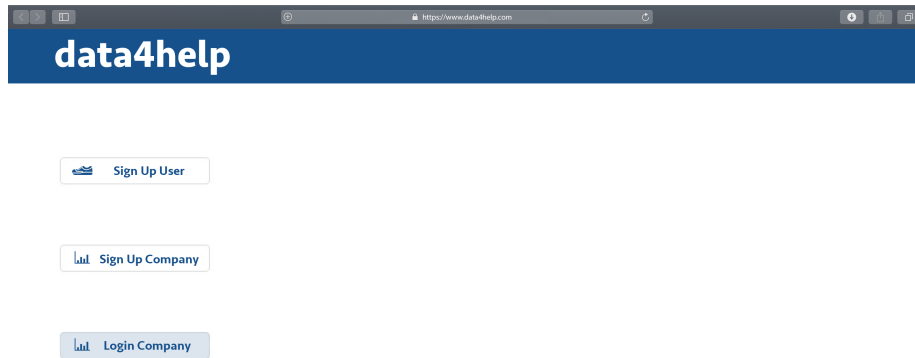
- [D5] Users sign up with their Google or Apple account.
- [D6] Users position is determined by using the GPS inside the smartwatch.
- [D7] When the system shows the position of a user it means that the user is actually there.
- [D8] During the registration process the user inserts his main data (height, weight, age, place where he lives).
- [D9] The user has the physical characteristics that he inserted in the system.
- [D10] Smart watch connects directly to TrackMe and send the data acquired. Data4Help and AutomatedSOS run only on smart watch with internet access.
- [D11] The user is able to accept or reject the following requests by clicking a button on the email that TrackMe sends to him.
- [D12] Every time that a user accept or reject a following request a notification is sent to Data4Help.
- [D13] Companies have a username and a vat number and they are unique.
- [D14] Data4Help is able to anonymize data based on the group request only if the group has more than 1000 users.
- [D15] Companies know the SSN of the user.
- [D16] A company that can see the data of a single user or of a group of users must also be able to choose the option that allows it to see users' data as soon as they are produced.

3 Specific Requirements

3.1 External interface requirements

3.1.1 User interfaces

Homepage.



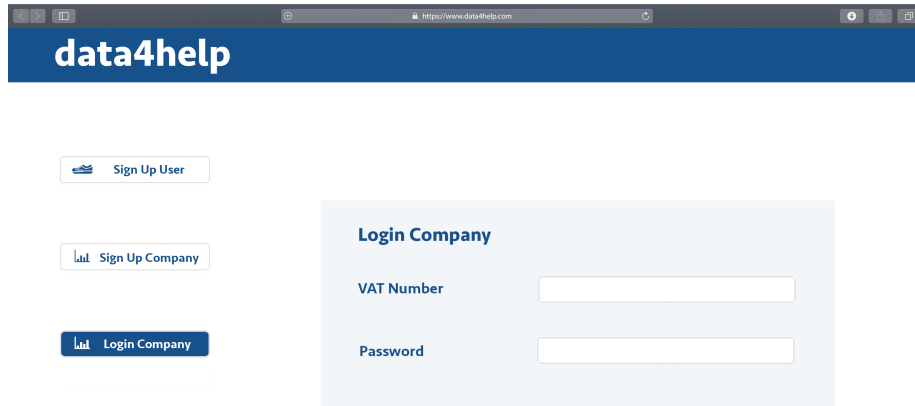
User sign up.

The screenshot shows a web browser window with the URL <https://www.data4help.com>. The header is a dark blue bar with the text "data4help" in white. On the left side, there is a vertical menu with three buttons: "Sign Up User" (highlighted in dark blue), "Sign Up Company" (light blue), and "Login Company" (light blue). The main content area is a light blue box titled "Sign Up User". It contains six input fields with labels: "Account iOS / Google", "Account Password", "SSN", "Place of Residence", "Height", and "Weight".

Company sing up.

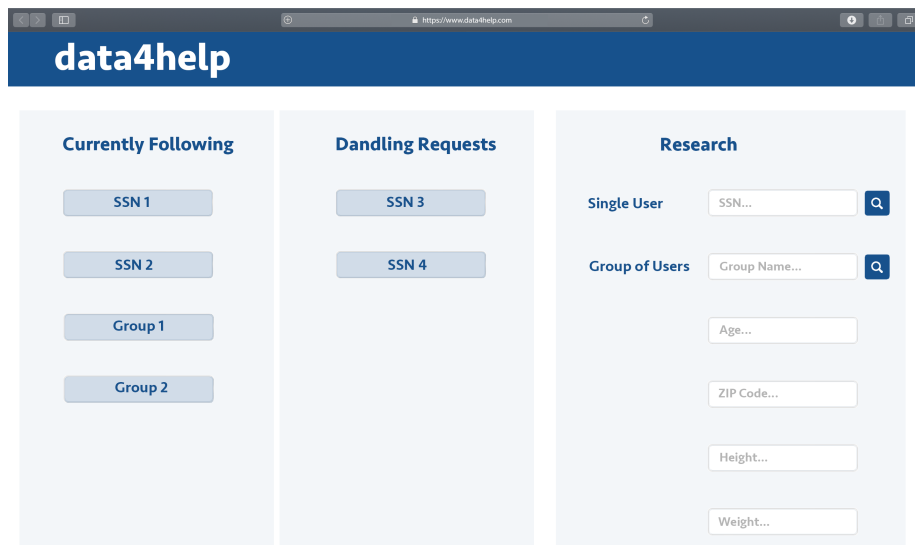
The screenshot shows the same web browser window as the previous one, but the "Sign Up Company" button in the left menu is now highlighted in dark blue. The main content area is a light blue box titled "Sign Up Company". It contains four input fields with labels: "Company Name", "VAT Number", "e-mail", and "Password".

Company login.



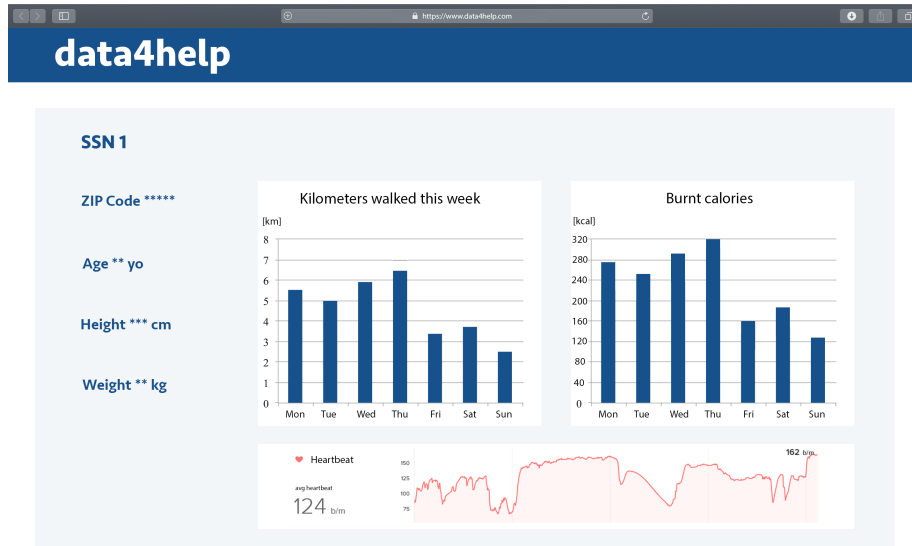
The screenshot shows the data4help website with a dark blue header containing the logo. On the left, there are three buttons: 'Sign Up User' (with a person icon), 'Sign Up Company' (with a building icon), and 'Login Company' (with a building icon and a dark blue background). To the right, a light blue box titled 'Login Company' contains two input fields: 'VAT Number' and 'Password'.

Requests.



The screenshot shows the data4help website with a dark blue header containing the logo. Below the header, there are three main sections: 'Currently Following', 'Dandling Requests', and 'Research'. The 'Currently Following' section has four buttons: 'SSN 1', 'SSN 2', 'Group 1', and 'Group 2'. The 'Dandling Requests' section has two buttons: 'SSN 3' and 'SSN 4'. The 'Research' section has two search bars: 'Single User' (with 'SSN...' as a placeholder) and 'Group of Users' (with 'Group Name...' as a placeholder). Below these are four more input fields: 'Age...', 'ZIP Code...', 'Height...', and 'Weight...'.

Single user's data.



Group users' data.



3.1.2 Hardware interfaces

- GPS
- Bluetooth
- Internet Connection
- Photoplethysmography (PPG)
- Accelerometer

3.1.3 Software interfaces

- Google Maps
- Ambulance Service

3.1.4 Communication interfaces

3.2 Scenarios

3.3 Functional requirements

3.3.1 [G1] Visitor can become User after providing credentials.

- [R1] The system must allow a visitor to begin the registration process. During the process the system will ask him to provide credentials.
- [D5] Users sign up with their Google or Apple account.
- [D8] During the registration process the user inserts his main data (height, weight, age, place where he lives).
- [D9] The user has the physical characteristics that he inserted in the system.

3.3.2 [G2] User can accept or reject the request of access to his data formulated by companies.

- [D1] The user's email is already known by TrackMe.
- [D11] The user is able to accept or reject the following requests by clicking a button on the email that TrackMe sends to him.
- [D12] Every time that a user accept or reject a following request a notification is sent to Data4Help.
- [R2] Each time that an accepting or rejecting notification is sent to Data4Help, the system must mark a *Pendent User* as not pendent anymore.
- [R3] Each time that a user changes state from pendent to non-pendent, the corresponding single user request in the company list moves from dandling to accepted.

3.3.3 [G3] If user's parameters are below specified thresholds, an ambulance is called within 5 seconds. [G3.1] Ambulance is required at current user's location.

- [R4] The system must be able to monitor the user heart rate through hardware interfaces that are installed in the smart watch.
- [D10] Smart watch connects directly to TrackMe and send the data acquired. Data4Help and AutomatedSOS run only on smart watch with internet access.
- [D6] Users position is determined by using the GPS inside the smartwatch.
- [D7] When the system shows the position of a user it means that the user is actually there.
- [D4] 5 seconds are necessary to send user location and call an ambulance when parameters are below the threshold.

3.3.4 [G4] Company can sign up as Company to Data4Help and AutomatedSOS.

- [R5] The system must allow a company to begin the registration process. During the process the system will ask to provide credentials.
- [D2] Only real companies can sing up as compaines.
- [R6] At the end of the registration process, the system must provide to the company a username and a password.
- [D13] Companies have a username and a vat number and they are unique.

3.3.5 [G5] Company can be recognized providing a password and vat number.

- [D13] Companies have a username and a vat number and they are unique.
- [R7] The company can log in to the website by providing the combination of a username and a password that match its account.

3.3.6 [G6] Company can formulate a request to see anonymized data of a group of users.

- [R8] The system must allow the company to formulate a group of users request.
- [R9] The system must allow the company to fill in the request via a drop down menu.
- [R10] The system must allow the company to send a notification to TrackMe software interfaces.

3.3.7 [G7] Company can formulate a request to see data of a specific user providing his SSN.

- [R11] The system must allow the company to formulate a single user request.
- [R12] The system must allow the company to fill in the request by inserting the user's SSN.
- [R10] The system must allow the company to send a notification to TrackMe software interfaces.

3.3.8 [G8] Company can see anonymized data of a group of users.

- [D3] Only companies can see users' data.
- [D14] TrackMe is able to anonymize data based on the group request only if the group has more than 1000 users.
- [R13] The system must allow companies to see the data that TrackMe was able to anonymize and for which exist the group request.

3.3.9 [G9] Company can see data of a specific user providing his SSN.

- [D3] Only companies can see users' data.
- [D15] Companies know the SSN of the user.
- [D16] The system must allow companies to see data of a single user if the single user request exists and if the user approved that request.

3.3.10 [G10] Company can subscribe to users' new data.

- [D3] Only companies can see users' data.
- [R14] The system must allow companies to see users' data as soon as they are produced.
- [D16] A company that can see the data of a single user or of a group of users must also be able to choose the option that allows it to see users' data as soon as they are produced.

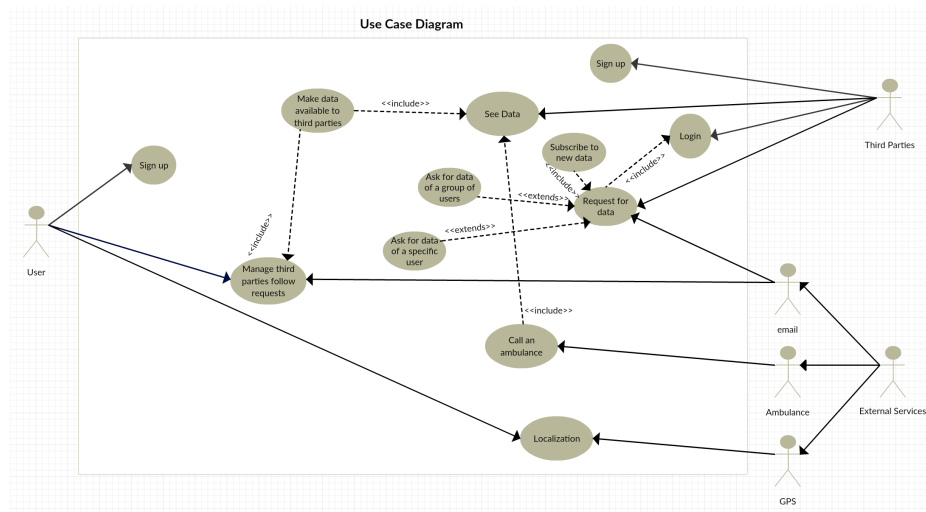
3.3.11 [G11] Data4Help can anonymise data.

- [D14] Data4Help is able to anonymize data based on the group request only if the group has more than 1000 users.
- [R15] The system must be able to anonymize data.

3.3.12 [G12] Data4Help can forward companies' requests to users.

- [D1] The user's email is already known by TrackMe.
- [R10] The system must allow the company to send a notification to TrackMe software interfaces.
- [R16] The system must allow TrackMe to send an email to the user in order to enable the company to see his data.

3.3.13 Use case diagram



Name	Visitor sing up.
Actors	User
Goals	[G1]
Input Conditions	There are no entry conditions.
Event Flow	<ol style="list-style-type: none"> 1. The user on the web home page clicks on the sign in button to start the registration process. 2. The user insert his Google account or Apple account. 3. The user fills all the mandatory fills. 4. The user clicks on the confirm button. 5. The system saves the data.
Output Conditions	The user successfully ends the registration process. From now on he can log into the application, providing his credentials and start using Data4Help.
Exceptions	<ol style="list-style-type: none"> 1. The user is already registered. 2. The user inserts no valid information in one or more mandatory fills. 3. The user chooses a username that has already been taken. 4. The user chooses an email that his associated with another user. 5. The user chooses a Google account or Apple account that is already used. <p>All the exceptions are handled notifying the issues to the user and taking back the event flow to point 2.</p>

Name	User accept or reject third party requests.
Actors	User
Goals	[G2]
Input Conditions	The user receives a request of following.
Event Flow	<ol style="list-style-type: none"> 1. The user checks his email and open the following request. 2. The user decides whether accepting it request or not, by clicking on one of the two button in the email.
Output Conditions	The user is notified to have actually accepted/reject the request. TrackMe is notified that a request has been accepted/rejected.
Exceptions	-

Name	Third part sign up.
Actors	Third part
Goals	[G4]
Input Conditions	There are no entry conditions.
Event Flow	<ol style="list-style-type: none"> 1. The third part on the home page clicks on the sign in button to start the registration process. 2. The third part fills all the mandatory fills. 3. The third part clicks on the confirm button. 4. The system saves the data.
Output Conditions	The third part successfully ends the registration process. From now on it can log into the application, providing his credentials and start using Data4Help and AutomatedSOS.
Exceptions	<ol style="list-style-type: none"> 1. The third part is already registered. 2. The third part inserts no valid information in one or more mandatory fills. 3. The third part chooses a vat number that has already been taken. <p>All the exceptions are handled notifying the issues to the third part and taking back the event flow to point 2.</p>

Name	Third part login.
Actors	Third part
Goals	[G5]
Input Conditions	There third part is already in the homepage.
Event Flow	<ol style="list-style-type: none"> 1. The third part inserts its credentials in. 2. The third part clicks on the login button in order to access. 3. The system redirects the third part to his profile.
Output Conditions	The third part his successfully redirects to his profile.
Exceptions	<ol style="list-style-type: none"> 1. The third part insert a not vat number. 2. The third part insert a not valid password. <p>All the exceptions are handled notifying the issues to the user and taking back the event flow to point 1.</p>

Name	Third part formulate a request to access anonymized data of a group of users.
Actors	Third part
Goals	[G6]
Input Conditions	The third part is already logged in into the system.
Event Flow	<ol style="list-style-type: none"> 1. The third part clicks on the <i>group request</i>. 2. The request is filled using drop-down menu. Each drop-down menu is linked to a type of filter. By selecting a filter the company is able to better specify the composition of the group it is interested in. 3. The request is sent to TrackMe by clicking on <i>send</i> button.
Output Conditions	The request is sent to TrackMe and a message for the correct sending of the request is presented to the company.
Exceptions	-

Name	Third part formulate a request to access data of a specific user through is SSN.
Actors	Third part
Goals	[G7]
Input Conditions	The third part is already logged in into the system.
Event Flow	<ol style="list-style-type: none"> 1. The third part clicks on the <i>single user request</i>. 2. The request is filled with the user's SSN. 3. The request is sent to TrackMe by clicking on <i>send</i> button.
Output Conditions	The request is sent to TrackMe and a message for the correct sending of the request is presented to the company.
Exceptions	-

Name	Third part can access anonymized data of a group of users.
Actors	Third part
Goals	[G8]
Input Conditions	There third part is already logged into the system.
Event Flow	<ol style="list-style-type: none"> 1. The third part accesses the approved group requests section. 2. The third part selects an approved group request. 3. The system redirects the third part to the request result.
Output Conditions	The data requested by the third part are shown.
Exceptions	<ol style="list-style-type: none"> 1. The data requested aren't anonymous since the outcome of the request concerns less than 1000 users. <p>All the exceptions are handled notifying the issues to the third part and taking back the event flow to point 1.</p>

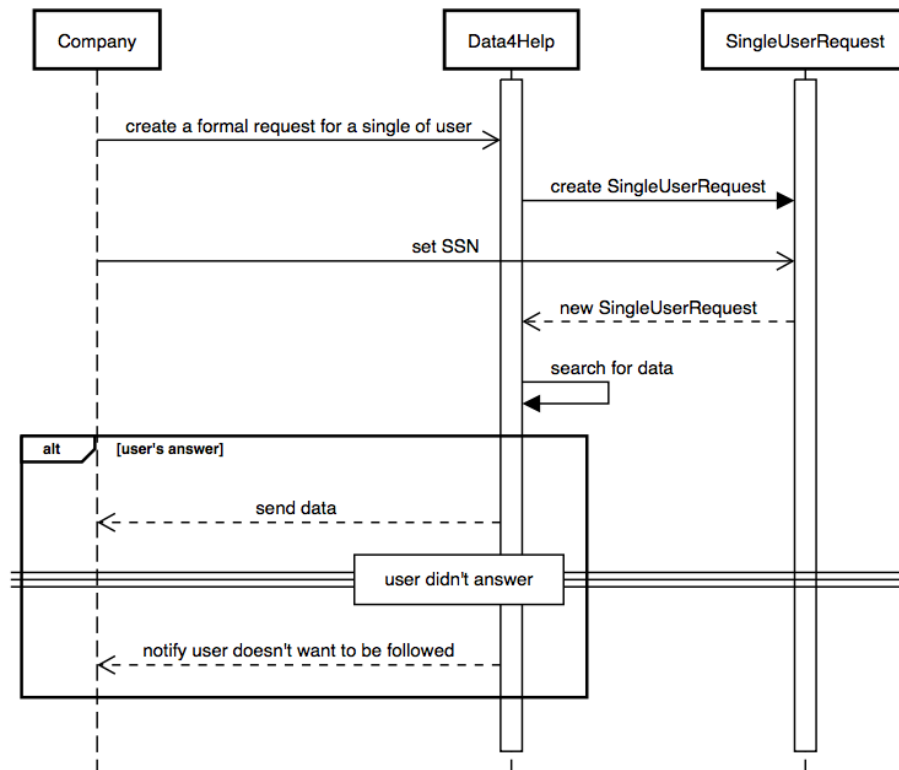
Name	Third part can access data of a specific user through his SSN.
Actors	Third part
Goals	[G9]
Input Conditions	There third part is already logged into the system.
Event Flow	<ol style="list-style-type: none"> 1. The third part accesses the approved single user requests section. 2. The third part selects an approved single user request. 3. The system redirects the third part to the request result.
Output Conditions	The data requested by the third part are shown.
Exceptions	<ol style="list-style-type: none"> 1. The user didn't approve the request. <p>All the exceptions are handled notifying the issues to the third part and taking back the event flow to point 1.</p>

Name	Data4Help can anonymise data.
Actors	TrackMe
Goals	[G11]
Input Conditions	Third part has requested data of a group of users.
Event Flow	<ol style="list-style-type: none"> 1. TrackMe performs the research among the matching users. 2. TrackMe anonymize the data of the selected users.
Output Conditions	The data requested from the third part are anonymized.
Exceptions	<ol style="list-style-type: none"> 1. The data requested aren't anonymous since the outcome of the request concerns less than 1000 users. <p>All the exceptions are handled notifying the issues to the third part and taking back the event flow to point 1.</p>

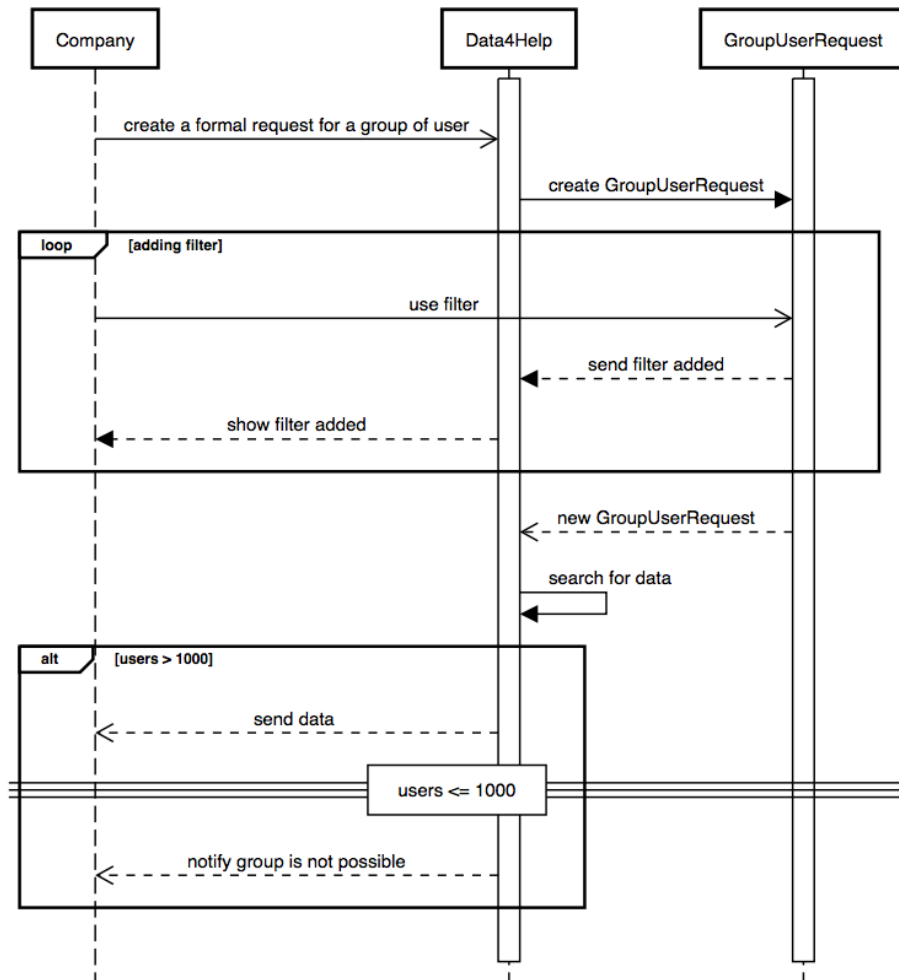
Name	TrackMe can forward third parties requests to users.
Actors	TrackMe
Goals	[G12]
Input Conditions	Third part has requested data of a single user.
Event Flow	<ol style="list-style-type: none"> 1. TrackMe forwards the request of being observed by a specific company to the user. 2. TrackMe marks the user as <i>pendent user</i>.
Output Conditions	The request of being followed by a company is sent to the user.
Exceptions	-

3.3.14 Sequence diagram

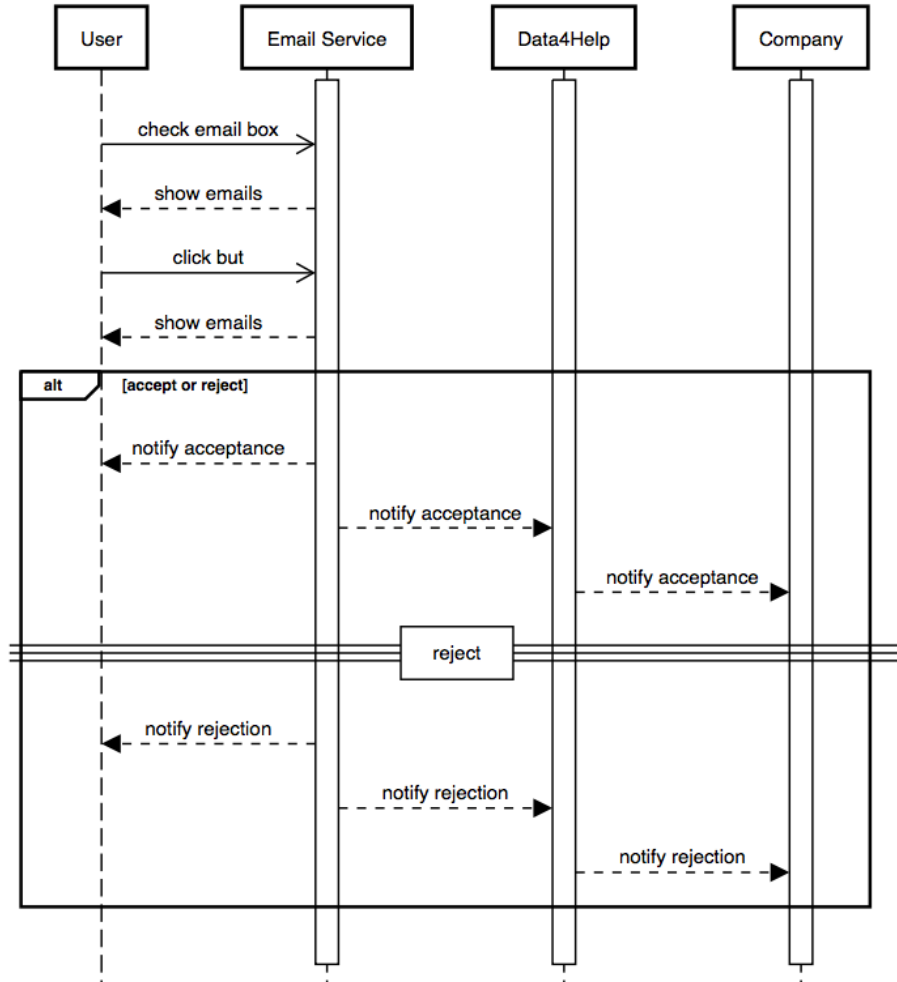
Company formulate single user request.



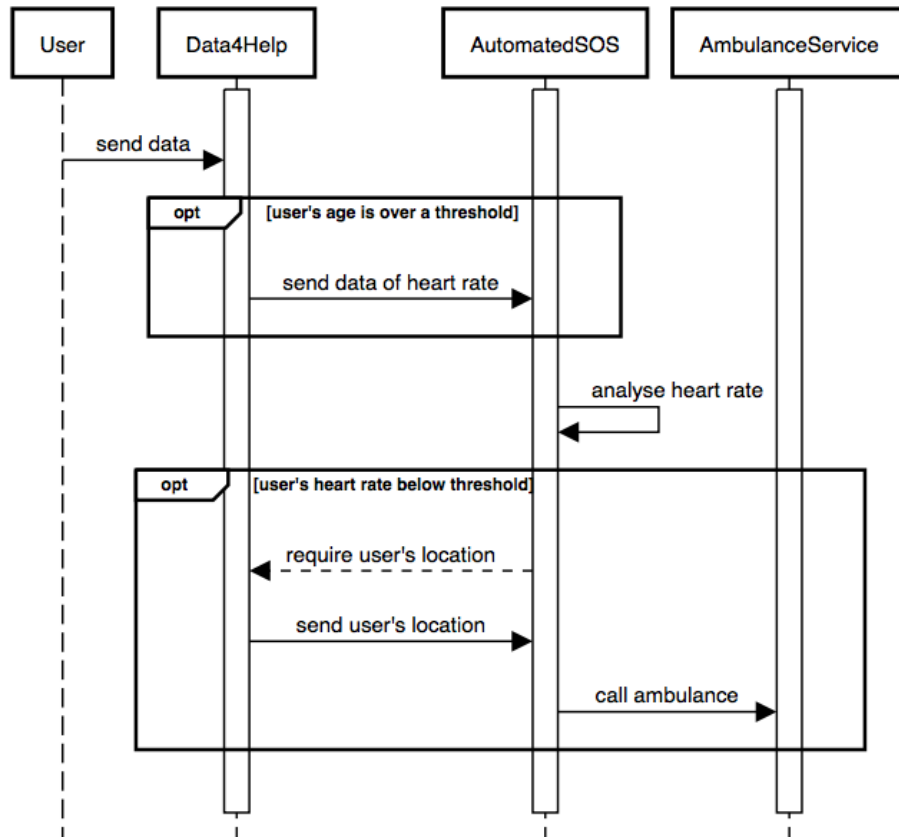
Company formulate group user request.



User accept or reject a following request.



AutomatedSOS calls an ambulance.



3.4 Performance requirements

- AutomatedSOS answers within 5 seconds.

3.5 Design constraints

3.5.1 Standard compliance

3.5.2 Hardware limitation

3.5.3 Other constraints

3.6 Software system attributes

3.6.1 Reliability

3.6.2 Security

3.6.3 Maintainability

3.6.4 Compatibility

4 Formal Analysis Using Alloy

4.1 Alloy model

4.2 World generated

4.3 Alloy results

5 Effort Spent

6 Resources