



# POLITECNICO

## MILANO 1863

### **TrackMe**

Requirements Analysis and Specification Document

Luca Conterio - 920261

Ibrahim El Shemy - 920174

A.Y. 2018/2019 - Prof. Di Nitto Elisabetta

# Contents

<b>1</b>	<b>Introduction</b>	<b>4</b>
1.1	Purpose . . . . .	4
1.2	Scope . . . . .	4
1.2.1	Goals . . . . .	5
1.3	Definitions, Acronyms and Abbreviations . . . . .	5
1.3.1	Definitions . . . . .	5
1.3.2	Acronyms . . . . .	5
1.3.3	Abbreviations . . . . .	6
1.4	Document Structure . . . . .	6
<b>2</b>	<b>Overall Description</b>	<b>7</b>
2.1	Product Perspective . . . . .	7
2.2	Product Functions . . . . .	9
2.3	User Characteristics . . . . .	9
2.4	Assumptions, Dependencies and Constraints . . . . .	9
2.4.1	Text Assumptions . . . . .	9
2.4.2	Domain Assumptions . . . . .	10
2.4.3	Dependencies and Constraints . . . . .	10
<b>3</b>	<b>Specific Requirements</b>	<b>11</b>
3.1	External Interface Requirments . . . . .	11
3.1.1	User Interfaces . . . . .	11
3.1.2	Third Party Interfaces . . . . .	13
3.1.3	Hardware Interfaces . . . . .	14
3.1.4	Software Interfaces . . . . .	14
3.1.5	Communication Interfaces . . . . .	14
3.2	Scenarios . . . . .	15
3.3	Functional Requirements . . . . .	17
3.4	Use Case Diagram . . . . .	20
3.5	Use cases . . . . .	21
3.5.1	Visitor Registration . . . . .	21
3.5.2	Third Party Registration . . . . .	21
3.5.3	User Login . . . . .	22
3.5.4	Third Party Login . . . . .	22
3.5.5	Request Assistance . . . . .	23
3.6	Performance Requirments . . . . .	23
3.7	Desgin Constraints . . . . .	23
3.7.1	Standards Compliance . . . . .	23
3.7.2	Hardware Limitations . . . . .	23

3.7.3	Other Constraints . . . . .	24
3.8	Software System Attributes . . . . .	24
3.8.1	Reliability . . . . .	24
3.8.2	Availability . . . . .	24
3.8.3	Security . . . . .	24
3.8.4	Maintainability . . . . .	24
3.8.5	Scalability . . . . .	24
<b>4</b>	<b>Formal Analysis Using Alloy</b>	<b>25</b>
<b>5</b>	<b>Effort Spent</b>	<b>26</b>
<b>6</b>	<b>Reference Documents</b>	<b>26</b>

# 1 Introduction

## 1.1 Purpose

This document represents the **Requirement Analysis and Specification Document** (RASD) for TrackMe software. Main goals of this project are to specify a system that will be able to store and analyze users' health data and whereabouts, to grant third parties to access these data or to subscribe to new data of a specific individual or to retrieve them, and to offer elderly people a rapid assistance based on their health parameters, if needed. At the same time, this document aims at describing the system through functional and nonfunctional requirements, to analyze customers' needs, to show the limits of the software, indicating the typical use cases that can occur.

## 1.2 Scope

TrackMe is a company that wants to develop a software-based service allowing third parties to monitor the location and health status of individuals. Hence, the system has to be composed by two specific services:

- **Data4Help**

This service supports the registration of individuals who agree that TrackMe acquires their data (through electronic devices such as smart-watches).

In addition, it supports the registration of third parties that can request:

- Access to the data of some specific individuals, who can accept/refuse it.
- Access to anonymized data of groups of individuals. These requests are approved by TrackMe if it is able to properly anonymize the requested data. The request is rejected if it is way too specific.

As soon as a request for some certain data is approved, TrackMe makes the previously saved data available to the third party. Also, it allows the third party to subscribe to new data and to receive them as soon as they are produced.

- **AutomatedSOS**

This service is oriented to elderly people: monitoring their health status parameters, the system can send to the location of the customer an ambulance when some parameters are below certain thresholds, guaranteeing a reaction time of less than 5 seconds from the time the parameters get lower than the threshold.

### 1.2.1 Goals

- [G1]: Allow visitors to easily register in the system.
- [G2]: Allow users to simply share personal information/health parameters.
- [G3]: Allow third parties to access information shared by users.
  - [G3.1]: Allow third parties to access information of specific individuals (through an identifier).
  - [G3.2]: Allow third parties to access anonymized information of groups of individuals.
  - [G3.3]: Allow third parties to subscribe to new information of a specific individual and to receive it.
- [G4]: Allow third parties to monitor specific users' parameters.
- [G5]: Guarantee the elderly users to receive an immediate assistance by an ambulance in case of high risk disease.
- [G6]: Guarantee the preservation of the privacy of the users.

## 1.3 Definitions, Acronyms and Abbreviations

### 1.3.1 Definitions

### 1.3.2 Acronyms

- RASD: Requirements Analysis and Specification Document.
- API: Application Programming Interface.
- GPS: Global Positioning System.
- SMS: Short Message Service.
- ETA: Estimated Time Arrival.

- RAPS: Reliable Array of Partioned Service.
- SSN: Social Security Number.

### 1.3.3 Abbreviations

- [Gn]: n-goal.
- [Rn]: n-requirment.
- App: application.

## 1.4 Document Structure

This paper refers to the structure suggested by IEEE for RASD documents, with very slight modifications:

1. **Introduction:** the first section is a general description of the system's scope and its goals. It also includes the revision history of the document and its references. Definitions and abbreviations used along the paper are provided too.
2. **Overall Description:** this section includes shared phenomena, requirements and domain assumptions. It also clarifies users' needs.
3. **Specific Requirements:** this section includes all the requirments, both functional and non functional.
4. **Formal Analysis Using Alloy:** it includes the Alloy model of the described system.
5. **Effort Spent:** this section includes information about the hours spent to draft this document.
6. **References:** this section includes references about papers/documents used to support this document.

## 2 Overall Description

### 2.1 Product Perspective

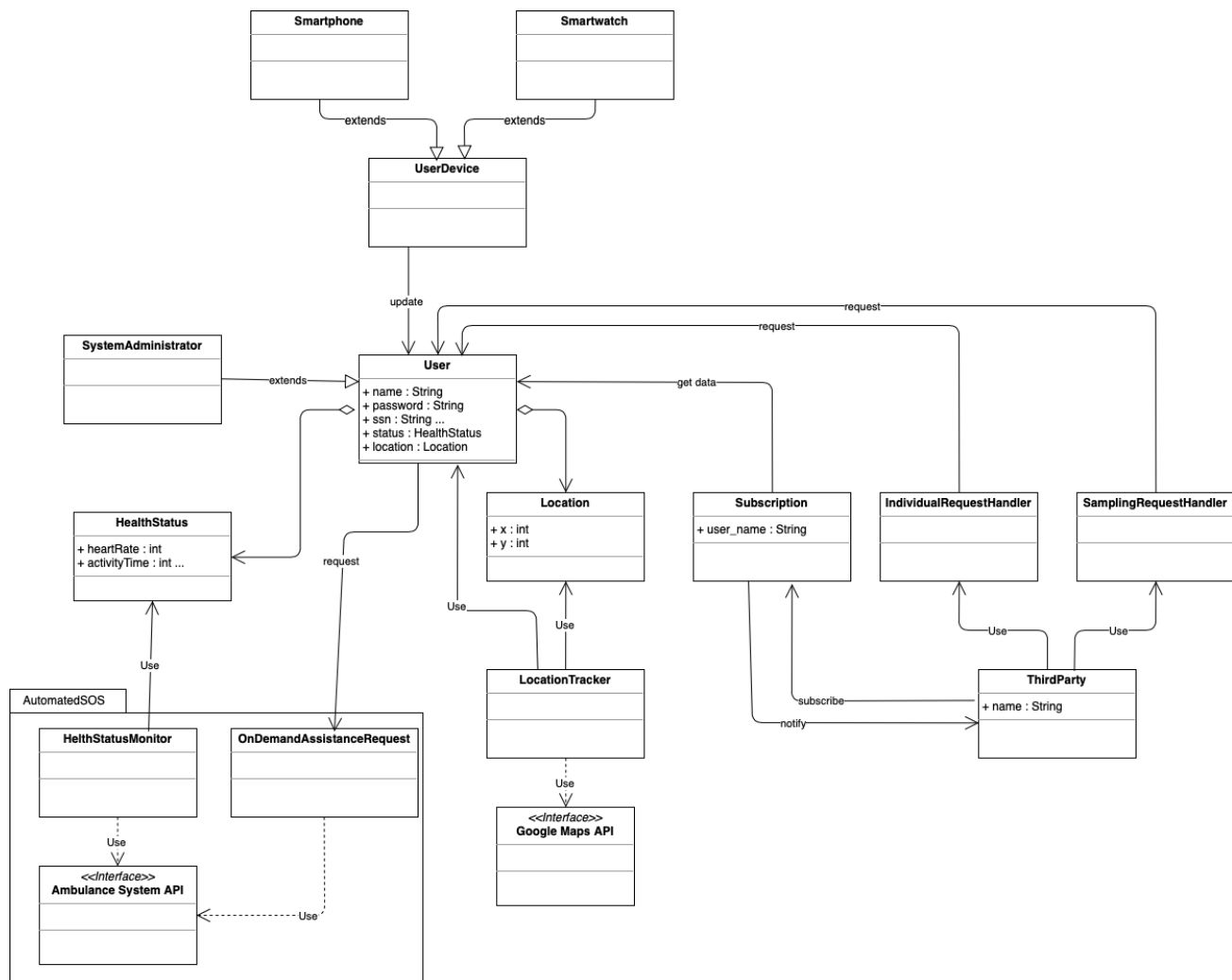


Figure 1: UML Class Diagram

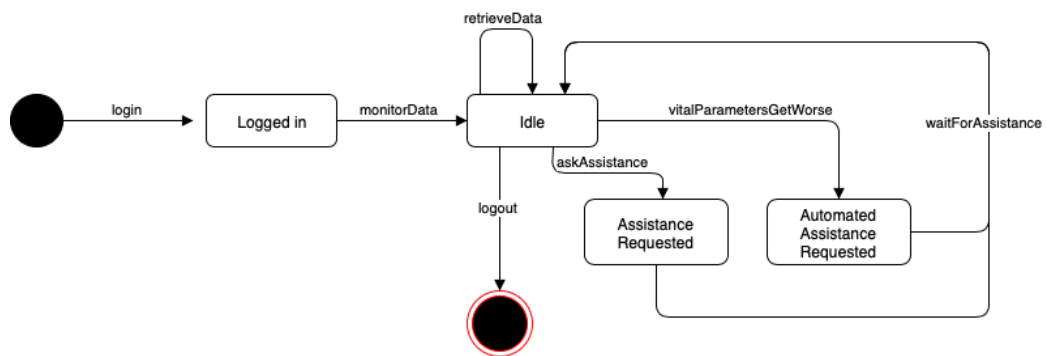


Figure 2: User Statechart Diagram

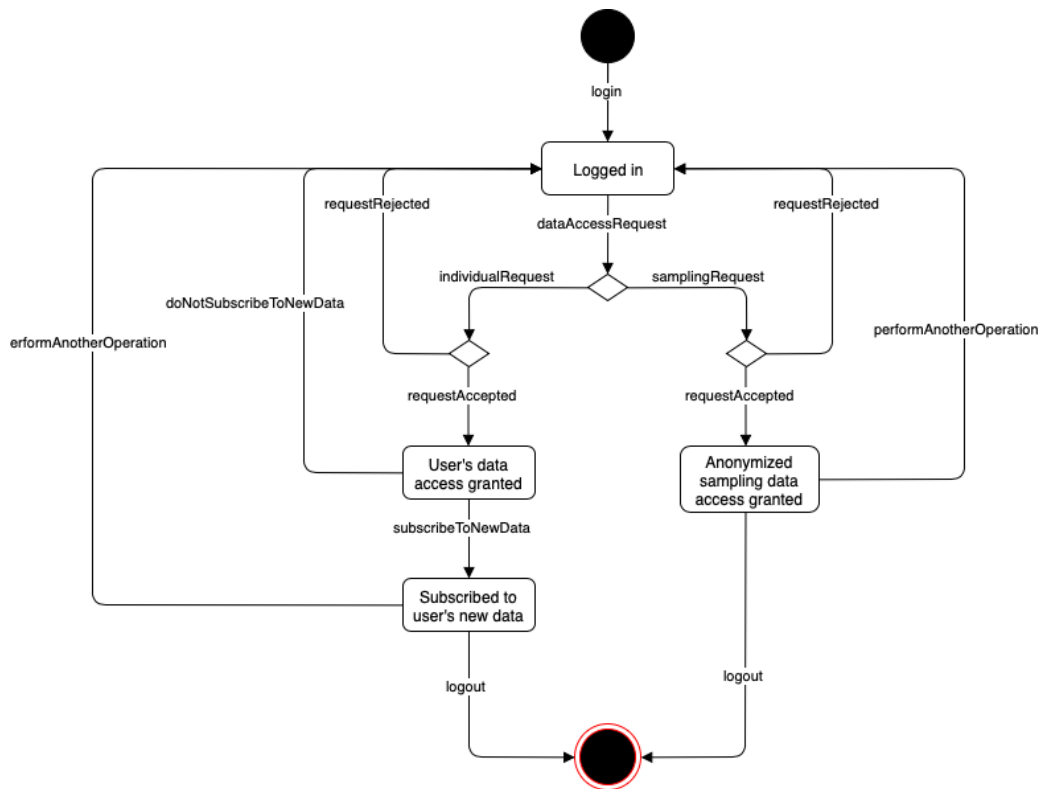


Figure 3: Third Party Statechart Diagram



## 2.2 Product Functions

## 2.3 User Characteristics

- **Visitor:** a person/third party visiting TrackMe without being registered. He can only proceed to registration in order to actually use system services, otherwise he can't have access to any service or data.
- **System Administrator:** doesn't require to register himself. Makes sure there are no issues in the interaction between users and third parties, guaranteeing a certain level of security.
- **Registered User:** called simply **user** in this document. A person who registered himself to TrackMe, sharing his personal data. He can login to the system through provided credentials to exploit full services.
- **Third Party User:** called simply **third party** in this document. A company or individual using the platform for some statistical goal or to offer assistance to registered users.
- **Ambulance Dispatcher:** called simply **dispatcher** in this document. An external individual to the system, whose role is to dispatch an ambulance to assist specific users.

## 2.4 Assumptions, Dependencies and Constraints

### 2.4.1 Text Assumptions

- In order to get registered, a Visitor must provide the following data: Name, Surname, Social Security Number, Date of Birth, Mobile Number, e-mail.
- Registration must be confirmed through a security code sent by SMS.
- Users are assumed to provide correct personal data (Name, Date of Birth, Social Security Number, etc.).
- Users are assumed to provide a valid Mobile Number and e-mail.
- Users' devices must support the Mobile Application.
- Users' devices must support the GPS technology.
- Users provide correct clinical data (such as blood group, allergies, etc.).

### 2.4.2 Domain Assumptions

- [D1]: The Social Security Number is be unique.
- [D2]: The verification message sent by SMS/e-mail will be certainly received by the User/Third Party.
- [D3]: Users' devices are up and running in order to retrieve and process data.
- [D4]: Data periodically received by Users' devices are assumed to have a good accuracy.
- [D5]: Data provided by Users' are assumed to be correct.
- [D6]: Users' devices support the GPS technology.
- [D7]: Users' devices support the Mobile Application.
- [D8]: Users' devices communicate through the Internet.
- [D9]: In case of emergency, all parameters relative to a specific individual are correctly reported to the Ambulance Dispatching System.
- [D10]: The Ambulance Dispatching System is always running and available.
- [D11]: The time spent by an ambulance to reach a defined location is as low as possible.

### 2.4.3 Dependencies and Constraints

1. Regulatory Policies: Guarantee confidentiality of information.
2. Hardware Limitations: ??? moved below
3. Interfaces to other Applications: ??? moved below

## 3 Specific Requirements

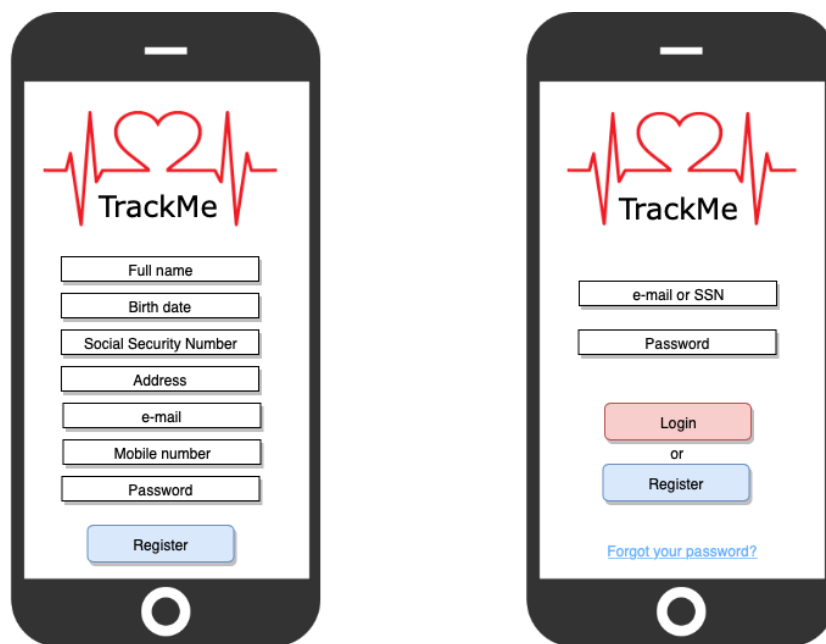
### 3.1 External Interface Requirments

The following mockups represent a basic idea of how the Mobile Application and the Web Interface are supposed to look like.

Users can access to complete TrackMe functionalities through the smart-phone application, while the smartwatch one will only support a subset of the system's services.

On the other side, TrackMe provides a Web Interface for Third Parties. Here they can exploit all the functionalities at their disposal, such as the request of a sampling according to some parameters.

#### 3.1.1 User Interfaces



The image displays two mobile application mockups side-by-side. Both screens feature a red heart icon with a pulse line and the text 'TrackMe' at the top. The left screen is the registration form, containing input fields for 'Full name', 'Birth date', 'Social Security Number', 'Address', 'e-mail', 'Mobile number', and 'Password', followed by a blue 'Register' button. The right screen is the login page, containing input fields for 'e-mail or SSN' and 'Password', followed by a red 'Login' button, the text 'or', a blue 'Register' button, and a blue link 'Forgot your password?' at the bottom.

Figure 4: Mobile App registration form and login page.



Figure 5: Mobile App homepage with activity data and AutomatedSOS interface during an ambulance request.

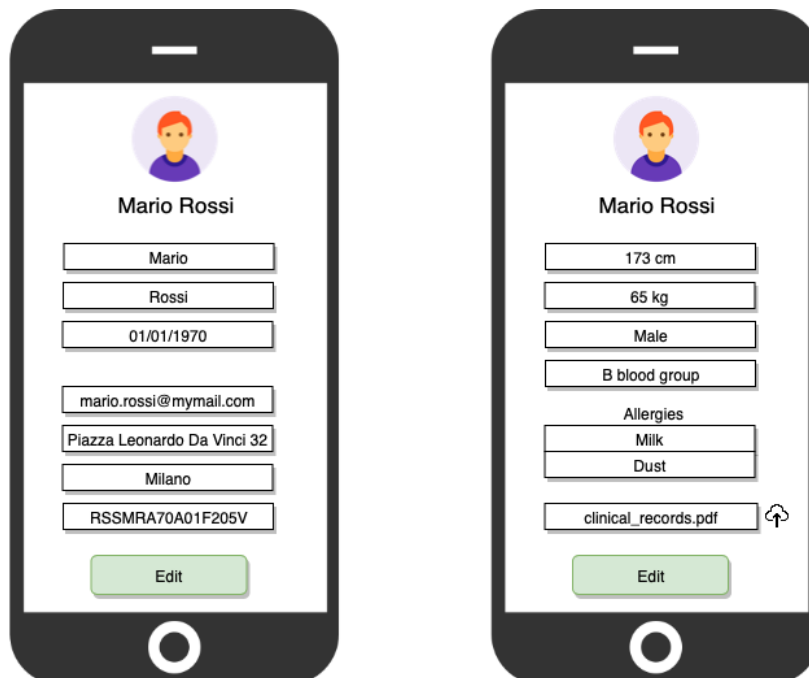


Figure 6: Personal data and clinical data pages.



Figure 7: Smartwatch App homepage with activity data, heartbeat testing page and AutomatedSOS interface during an ambulance request.

### 3.1.2 Third Party Interfaces

### **3.1.3 Hardware Interfaces**

### **3.1.4 Software Interfaces**

TrackMe will make use of some Application Programming Interfaces to simplify the implementation, since these components are largely used and compatible with the majority of the devices currently on the market:

- Google Maps API to have a visual representation of user location and to get it in critical moments, such as AutomatedSOS requests to the Ambulance Dispatching System.
- Google Fit Sensors API to read raw sensor data in real time. It allows listing the available sensors on the device on which the application is running and registering a listener on specific sensors to retrieve data automatically.
- Ambulance Dispatching System API to perform assistance requests. Actually it could be an automatic phone call to the ambulance contact center, during which an algorithm communicates all relevant data to the interlocutor (e.g. name, age, location etc.).

### **3.1.5 Communication Interfaces**

Since the TLS versions 1.0 and 1.1 will not be more supported, TrackMe must rely on the newer TLS version 1.3, released in 2018, to guarantee the best security possible, at least during the HTTPS connections involving messages carrying credentials or other sensible data. For other types of connections, e.g. to retrieve periodical data from users' devices, TCP persistent connections can be avoided: even if a packet is lost another one will be generated within a slight amount of time, so UDP non-persistent connections can be used (it is a stream of data). This can also provide a lower server load, as pointed out later in section 3.6, Performance Requirements.

## **3.2 Scenarios**

### **Scenario 1 - Registration**

Marco saw the advertisement of TrackMe and decided to download the mobile application in order to exploit in a useful way his new smartwatch. After opening the new app, it is asked to fill a form with all his personal information, full name, date of birth, mobile number, SSN, etc. To proceed with his registration, after all fields have been filled, Marco clicks on the "Register" button and, as soon as he does, he receives an SMS on his mobile phone confirming the positive outcome of his operation. Marco is now a Registered User of TrackMe: he can login to update his clinical information and benefit of all functionalities of the application.

### **Scenario 2 - Automatic Ambulance Request**

Maria is a 76 years old User of TrackMe, so she can benefit of the AutomatedSOS service. Thanks to this functionality the system checks periodically her heart rate. During a relax time, Maria's heart rate get so low that her heart risks to stop. Luckily she always wears a smartwatch on her wrist, because she's aware of the utility and importance of TrackMe's monitoring. In fact, as soon as her heart rate gets lower than 30 bpm, AutomatedSOS sends an assistance request to the Ambulance Dispatching System, notifying Maria about the estimated time of arrival of the aid team.

### **Scenario 3 - On-Demand Ambulance Request**

A sport addicted user such as Jhon always goes out during the morning to have a run in the park. In the last period he didn't have time to train himself so much as before and now he has more difficulties. Coming back to home, he starts feeling weak. He measure his pressure values and notice that they are lower than their normal level. To speed up the operation and to avoid calling the ambulance service, he logs in his TrackMe account and in the homepage he clicks on "Request assistance". The application confirms that the request has been successfully sent and updates Jhon about the Estimated Time of Arrival of the ambulance.

### **Scenario 4 - Search for a User**

### **Scenario 5 - Anonymous Sampling**

ItalianStatistica is a big company that performs statistical analysis on the italian territory studying the differences between some geographical areas.

For a new analysis on Milan's population, ItalianStatistica decides to retrieve samples from the Data4Help database. After the registration the company can perform anonymous samplings on the people living in Milan. Since asking for how many people with blue eyes and younger than 15 live in the city center results in sampling than 1000 individuals, Data4Help refuses such a request. In order to produce a sampling, ItalianStatistica extends the search to the entire municipality. In this way, a group of more than 1000 individuals is found and the sample with all relevant data is made accessible to the company.



### 3.3 Functional Requirements

#### **[G1]: Allow visitors to easily register in the system**

- [D1]: The Social Security Number is be unique.
- [D2]: The verification message sent by SMS/e-mail will be certainly received by the User/Third Party.
- [R1]: The system must allow the Visitor/Third Party to provide credentials and personal data.
- [R2]: The system must verify the correspondance between the SSN provided by the Visitor/Third Party and their personal information.
- [R3]: The system must verify the correctness of the data provided by the Visitor/Third Parties with an e-mail/SMS verification.
- [R4]: The system must verify that there are no other registered Users/Third Parties with the same e-mail/SSN.
- [R5]: In order to register successfully a Third Party, the system must oblige it to accept users data privacy conditions.

#### **[G2]: Allow Users to share personal information/health parameters**

- [D3]: Users' devices are up and running in order to retrieve and process data.
- [D4]: Data periodically received by Users' devices are assumed to have a good accuracy.
- [D5]: Data provided by Users' are assumed to be correct.
- [D6]: Users' devices support the GPS technology.
- [D7]: Users' devices support the Mobile Application
- [D8]: Users' devices communicate throught the Internet.
- [R6]: Users locations must be retrieved by GPS.
- [R7]: The system must allow the Users to update their personal data.
- [R8]: The system must allow the Users to upload their medical records (such as blood group).

**[G3]: Allow Third Parties to access information shared by the Users**

- [G3.1]: Allow Third Parties to access information of specific individuals.
  - [R9]: The system must allow Third Parties to search Users through their SSN's.
  - [R10]: The system must allow Third Parties to send requests in order to access specific data.
  - [R11]: The system must allow Users either to accept or refuse Third Parties' requests.
- [G3.2]: Allow Third Parties to access anonymized information and parameters of groups of individuals.
  - [R12]: The system must allow Third Parties to perform samplings according to some parameters (such as Geographical ones).
  - [R13]: The system must anonymize sampling result data.
  - [R14]: The system must accept sampling if and only if results are related to more than 1000 Users.
- [G3.3]: Allow Third Parties to subscribe to new information of a specific individual and to receive it.
  - [R15]: If a User accepts a requests, the system must allow Third Parties to store and access the previously saved data.
  - [R16]: The system must show Third Parties new data whenever they are available.

**[G4]: Guarantee the elderly users to receive an immediate assistance by an ambulance in case of high risk disease**

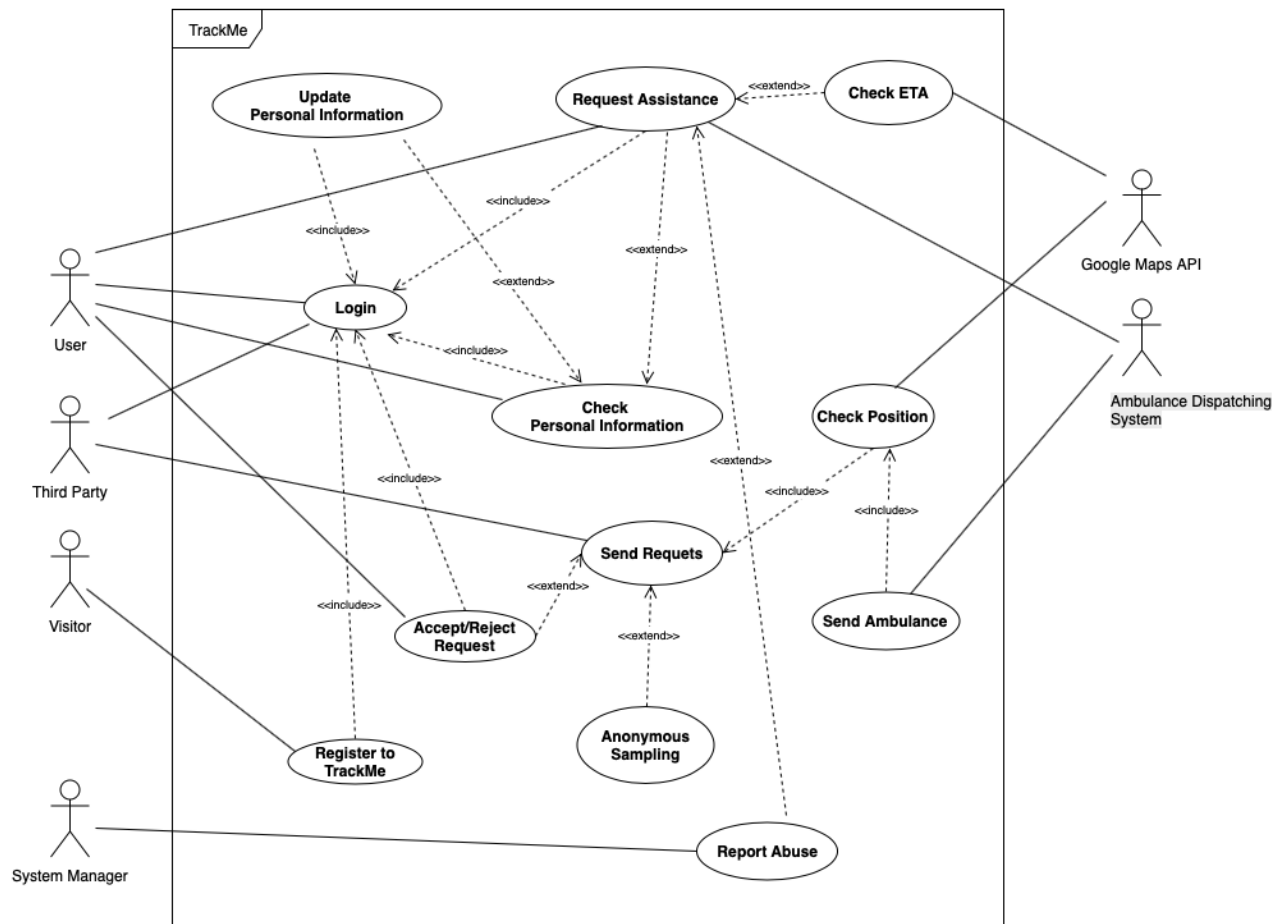
- [D4]: Data periodically received by Users' devices are assumed to have a good accuracy.
- [D9]: In case of emergency, all parameters relative to a specific individual are correctly reported to the Ambulance Dispatching System.
- [D10]: The Ambulance Dispatching System is always running and reliable.

- [D11]: The time spent by an ambulance to reach a defined location is as low as possible.
- [R16]: The AutomatedSOS service is automatically activated during the registration process if the Visitor is over 60.
- [R17]: The Health Status Monitoring System must notify the Ambulance Dispatching System as soon as possible (within 5 seconds).
- [R18]: When the Ambulance Dispatching System is notified, the Health Status Monitoring System sends all the User's clinical parameters.
- [R19]: The system should let the User have the possibility to request directly help from an ambulance if he/she feels it is necessary.
- [R20]: Users' devices must support sensors for retrieving health parameters.

**[G5]: Guarantee the preservation of the privacy of the Users.**

- [D4]: Data periodically received by Users' devices are assumed to have a good accuracy.
- [D5]: Data provided by Users' are assumed to be correct.
- [R5]: In order to register successfully a Third Party, the system must oblige it to accept data privacy conditions.
- [R14]: The system must accept sampling if and only if results are related to more than 1000 Users.
- [R21]: A Third Party can access data and parameters of a specific User if and only if he/she accepts the request.
- [R22]: The system must implement some form of accurate access control on databases.

### 3.4 Use Case Diagram



### 3.5 Use cases

#### 3.5.1 Visitor Registration

NAME	Register to TrackMe
ACTOR	Visitor
GOALS	[G1]
ENTRY CONDITIONS	The Visitor must have installed the Application on his/her Mobile device
EVENTS FLOW	1. Fill all mandatory fields in the Registration form 2. Click on "Register" button 3. System checks data validity 4. System sends an SMS as confirmation 5. System saves Users' data
EXIT CONDITIONS	The Vistor has successfully registered to TrackMe
EXCEPTIONS	1. The User is already registered 2. The e-mail is already registered 3. The Mobile Number is already registered 2. The SSN provided is invalid 3. Some mandatory fields are not filled

#### 3.5.2 Third Party Registration

NAME	Register to TrackMe
ACTOR	Third Party
GOALS	[G1]
ENTRY CONDITIONS	The Third Party must have installed the Application on its Mobile device
EVENTS FLOW	1. Fill all mandatory fields in the Registration form 2. Click on "Register" button 3. System checks data validity 4. System sends an SMS as confirmation 5. System saves Third Party's data
EXIT CONDITIONS	The Third Party has successfully registered to TrackMe
EXCEPTIONS	1. The Third Party is already registered 2. The e-mail is already registered 3. The Mobile Number is already registered 2. The SSN provided is invalid 3. Some mandatory fields are not filled

### 3.5.3 User Login

NAME	Login
ACTOR	User
GOALS	[G1]
ENTRY CONDITION	The Visitor must be in the Login page
EVENTS FLOW	1. Enter e-mail or SSN 2. Enter the password 3. Click on "Login" button
EXIT CONDITIONS	The User has successfully logged in
EXCEPTIONS	1. The User is not registered 2. The e-mail is wrong 3. The SSN is wrong 2. The password is wrong 3. Some mandatory fields are not filled

### 3.5.4 Third Party Login

NAME	Login
ACTOR	Third Party
GOALS	[G1]
ENTRY CONDITION	The Third Party must be in the Login page
EVENTS FLOW	1. Enter e-mail or SSN 2. Enter the password 3. Click on "Login" button
EXIT CONDITIONS	The Third Party has successfully logged in
EXCEPTIONS	1. The Third Party is not registered 2. The e-mail is wrong 3. The SSN is wrong 2. The password is wrong 3. Some mandatory fields are not filled

### 3.5.5 Request Assistance

NAME	Request Assistance
ACTOR	User
GOALS	[G1]
ENTRY CONDITION	The User must be in the HomePage
EVENTS FLOW	1. Click on "Request Assistance" button 2. Confirm the operation when it is asked.
EXIT CONDITIONS	The User has successfully requested Assistance
EXCEPTIONS	GPS is not active on User's device

## 3.6 Performance Requirments

The system must be able to handle a huge quantity of requests simultaneously throughout the day, responding to users' necessities in the shortest time possible. In order to improve the perfomance of the system, since data are received in a discrete way (e.g. monitored every 5 seconds), TrackMe relies on a UDP non-persistent connection.

For what concerns the AutomatedSOS service, it is required that each ambulance request is generated and sent to the Ambulance Dispatching System within 5 seconds from the moment in which the vital parameters of an elder user get below the fixed threshold.

## 3.7 Desgin Constraints

### 3.7.1 Standards Compliance

### 3.7.2 Hardware Limitations

- Mobile App: iOS/Android, Internet Connection, GPS.
- AppleWatch/WearOS: smartwatches linked to mobile devices or equipped with GPS and equipped with hearbeat/pressure sensors.
- Web App: browser (e.g. Google Chrome / Safari) able to retrieve users' location.

### **3.7.3 Other Constraints**

## **3.8 Software System Attributes**

### **3.8.1 Reliability**

The system must guarantee a 24/7 service. This requirement should not have any sort of deviation (especially concerning AutomatedSOS).

### **3.8.2 Availability**

The system must fulfil all the requests whenever needed (e.g. get/update personal information, request for medical assistance). Only a small percentage of the total requests is admissible (less than 0.01% of the total amount of requests). The system relies on a RAPS architecture, to better guarantee availability. The whole system is partitioned in nodes, each one managing a single service, in which data is made redundant in different servers. In this way, the malfunction of a service will not cause a service breakdown, but only a decrease of performance.

### **3.8.3 Security**

Despite the fact that personal information is stored, the system guarantees not to spread them outside, and third parties are obliged to be confirmed with a privacy policy.

### **3.8.4 Maintainability**

Enforced by the usage of specific design patterns (e.g. third party subscription is notified through an Observer Pattern whenever new data is generated by the users) and the provided documentation.

### **3.8.5 Scalability**

Relying on a RAPS architecture, it is easier to enlarge the structure of the system, since it is possible to invest only on those services that need to handle the higher amount of requests or the ones where the number of users is relevant.



## 4 Formal Analysis Using Alloy

## 5 Effort Spent

- Luca Conterio

Day	Subject	Hours
15/10/2018	Purpose, Scope and goals	1
18/10/2018	Overall Description	1.5
19/10/2018	User Interface sketch and Domain assumptions	2
22/10/2018	UML and Non-Functional Requirements	3.5
25/10/2018	Functional Requirements	3
26/10/2018	Statechart Diagrams	2
28/10/2018	User Interface and Scenarios	1.5
29/10/2018	Interfaces and Scenarios	1.5
Total		16

- Ibrahim El Shemy

Day	Subject	Hours
15/10/2018	Purpose, Scope and goals	1
18/10/2018	Overall Description	1
19/10/2018	Domain Assumptions	2
22/10/2018	Assumptions and Non-Functional Requirements	3.5
25/10/2018	Functional Requirements	3
26/10/2018	Functional Requirements	1
27/10/2018	Use Case Diagram	3
28/10/2018	Use Case Diagram and Use Cases	1
Total		15.5

## 6 Reference Documents

- Specification Document "Mandatory Project Assignment A.Y. 2018/2019"
- 830-1993 - IEEE Recommended Practice for Software Requirements
- "Appunti di Sistemi Informativi per il Settore dell'Informazione" A.Y. 2017/2018 Specifications