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

# 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 smartwatches).
  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

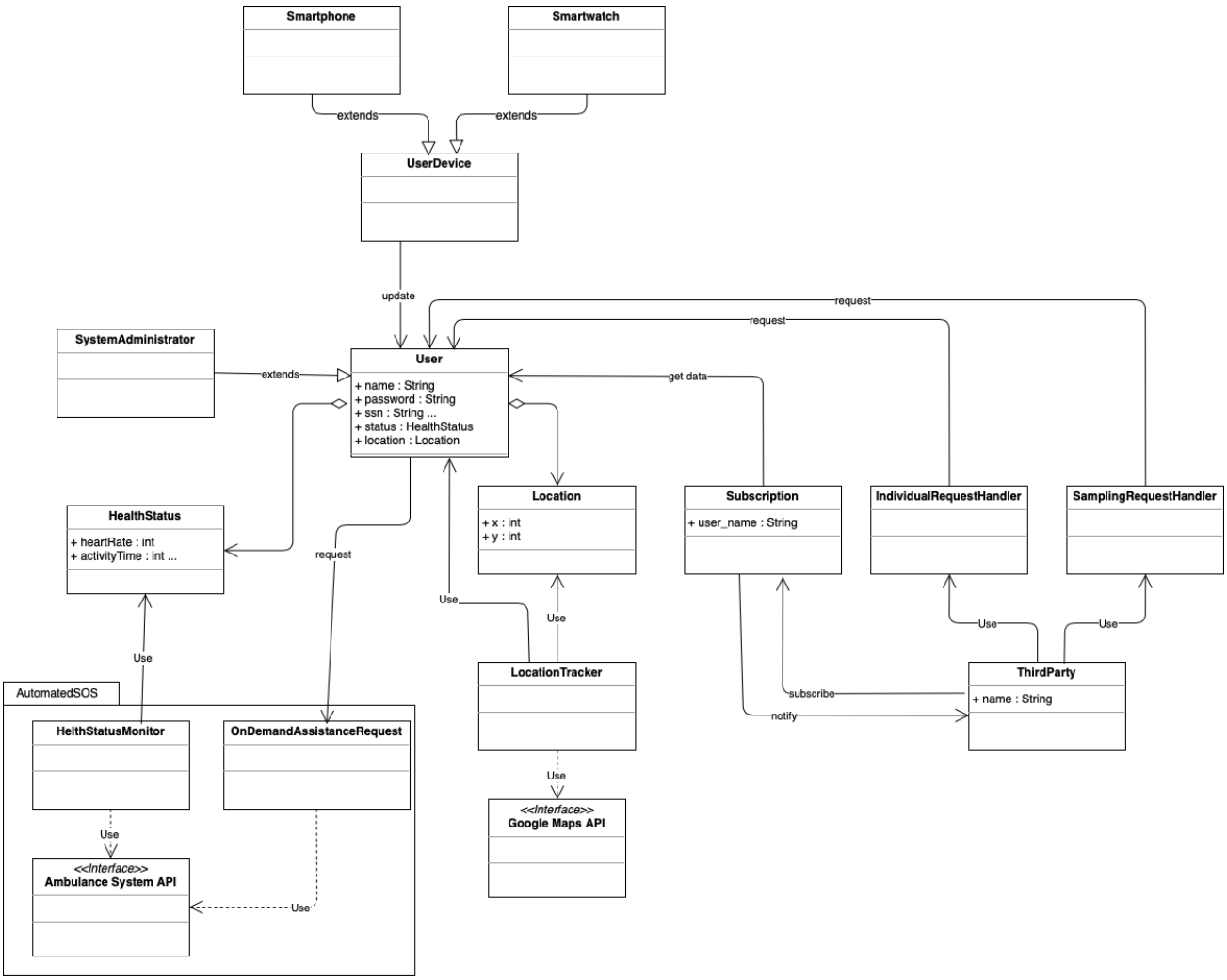



Figure 1: UML Class Diagram

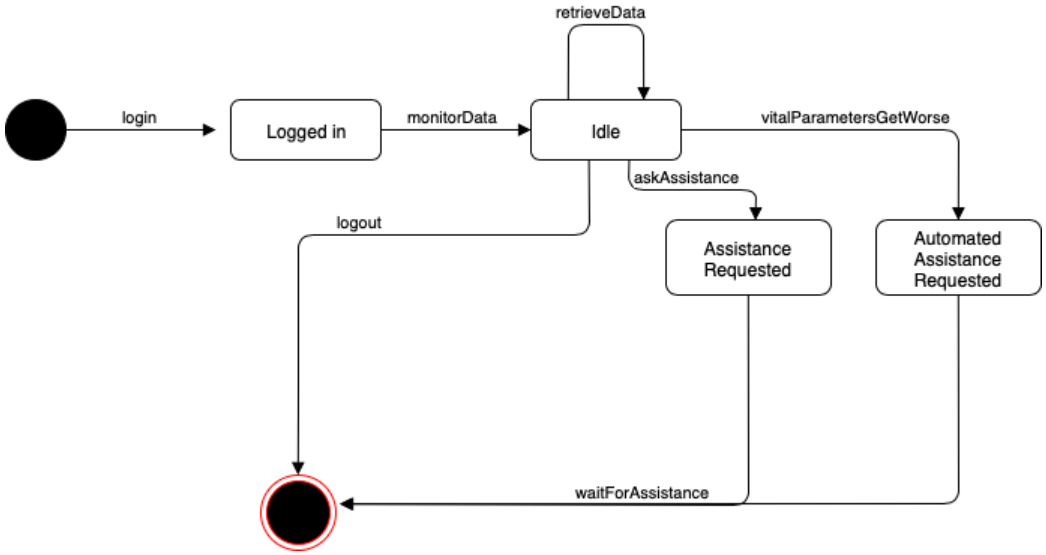



Figure 2: User Statechart Diagram

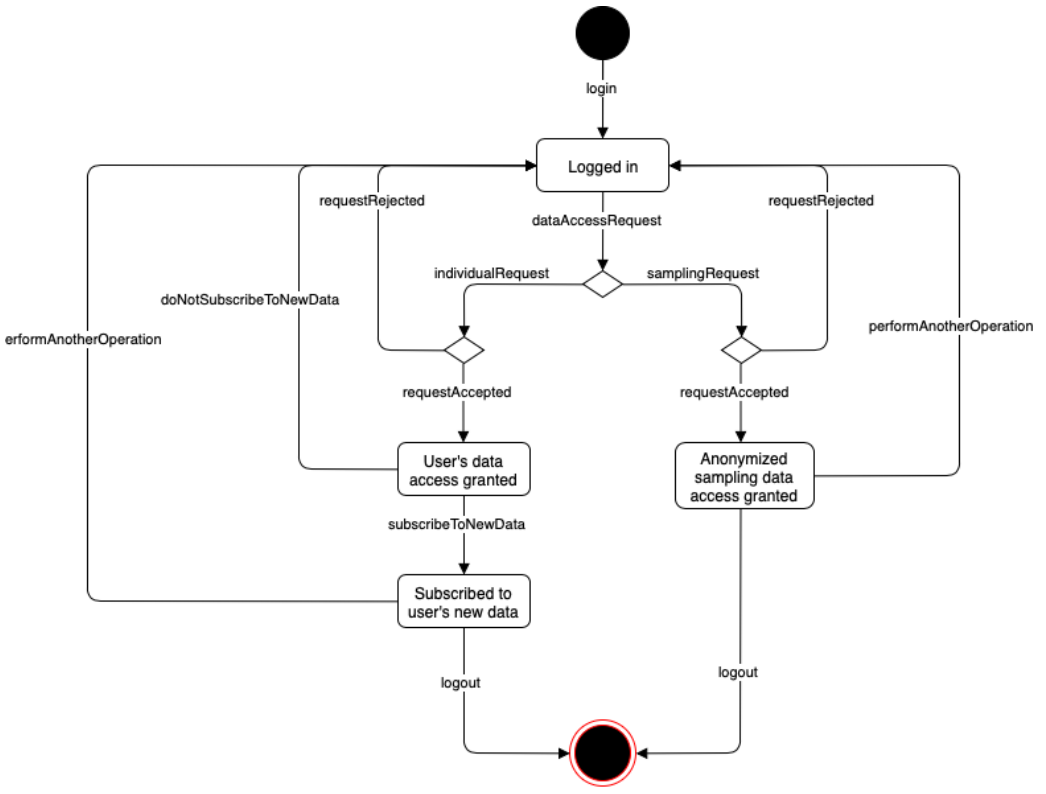



Figure 3: Third Party Statechart Diagram

## 2.2 Product Functions

## 2.3 User Characteristics

- `Visitor`: a person visiting TrackMe without being registered. He can only proceed to registration in oder 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 invidual 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.
- In order to get registered, 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**]: Social Security Number must be unique.
- [**D2**]: The verification message sent by SMS/e-mail will be certainly received by the User.
- [**D3**]: Users' devices are up and running in order to retrieve and process data.
- [**D4**]: Data received (such as current location) by users' mobile devices are assumed to be correct.
- [**D5**]: Users' devices must support the Mobile Application.
- [**D6**]: Parameters provided by Users' are assumed to be correct.
- [**D7**]: The time spent by an ambulance to reach a defined location must be as low as possibile.
- [**D8**]: Users' devices are assumed to 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 must be as low as possible.
- [**D12**]: The time spent by an ambulance to reach a defined location must be as low as possibile.

### 2.4.3 Dependencies and Constraints

1. Regulatory Policies: Guarantee confidentiality of information.
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. Interfaces to other Applications:

   - API to ambulance dispatching system.
   - API to external applications that monitor users health and activity parameters. (???)
   - Google Maps API to have a visual representation of user location.

# 3 Specific Requirements

## 3.1 External Interface Requirments

### 3.1.1 User Interfaces

The following mockups represt a basic idea of how the mobile application is supposed to look like.

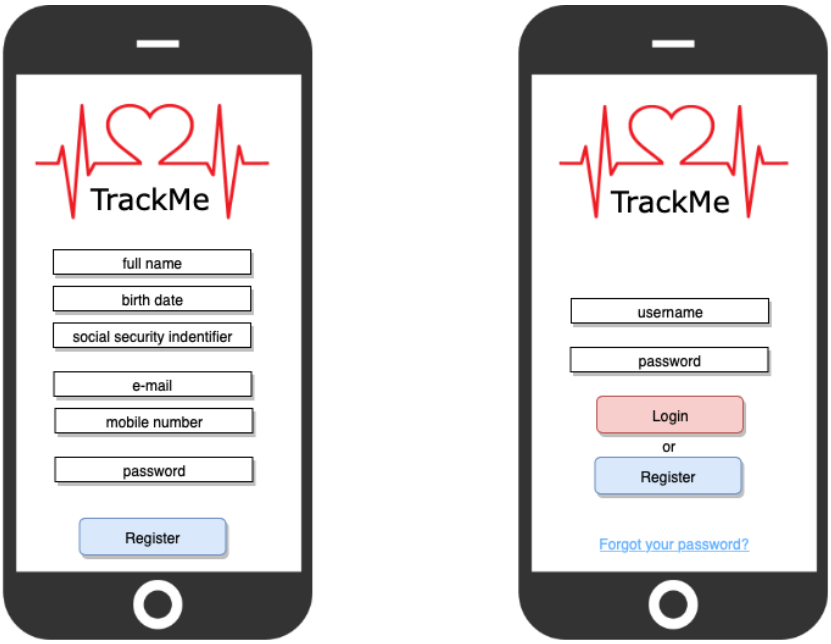



Figure 4: Mobile App Registration form and login page

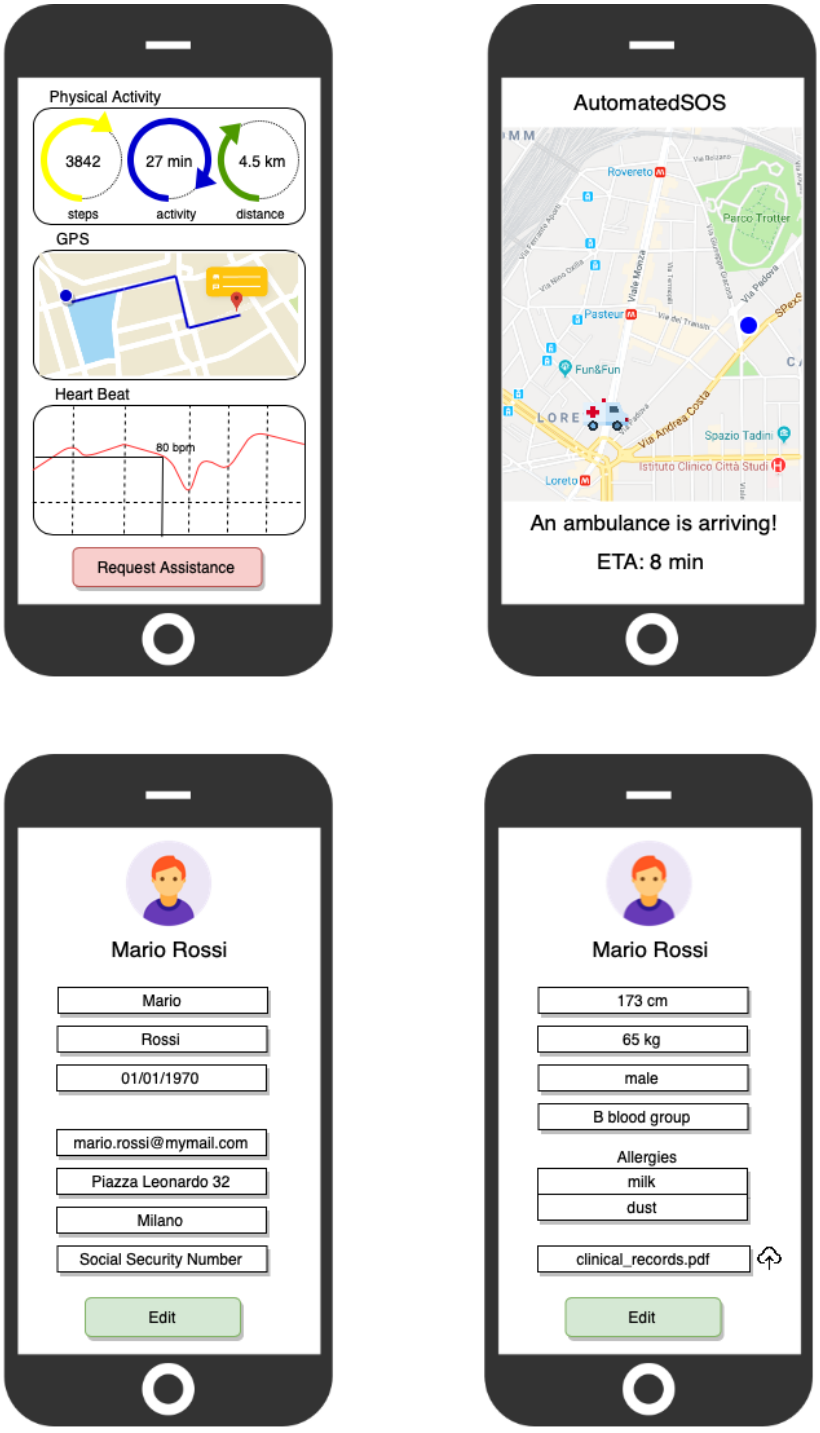



Figure 5: Mobile app homepage with activity data, AutomatedSOS interface during an ambulance request and personal data pages.

### 3.1.2 Hardware Interfaces

### 3.1.3 Software Interfacse

### 3.1.4 Communication Interfaces

## 3.2 Scenarios

## 3.3 Functional Requirments

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

- [D1]: The SSN must 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 SSN/e-mail.
- [R5]: In order to register successfully a Third Party, the system must oblige it to accept 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]: Users' devices must support the GPS technology.
- [D5]: Users' devices must support the Mobile Application
- [D6]: Data periodically received by Users' devices are assumed to have a good accuracy.
- [D7]: Parameters provided by Users' are assumed to be correct.
- [D8]: Users' devices are assumed to communicate throught the Internet.

- [R6]: Users locations are 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**

- [D6]: Parameters 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.

- [D12]: The time spent by an ambulance to reach a defined location must be as low as possibile.

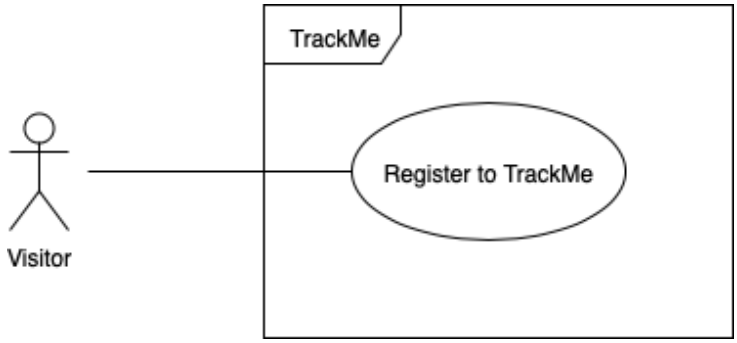
- [R16]: The AutomatedSOS service is automatically activated during the registration process if the Visitor is over 60.
- [R17]: The Health Status Monitoring System must notify the Ambulance Dispatching System.
- [R18]: When the Ambulance Dispatching System is notified, the Health Status Monitoring System sends all the User's clinical parameters.
- [R19]: The system should let the User have the possibily to request directly help from an ambulance if he feels it is necessary.

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

- [D2]: Parameters 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.
- [R8]: A Third Party can access data and parameters of a specific User if and only if he/she accepts the request.
- [R3]: The system must accept sampling if and only if results are related to more than 1000 Users.
- [R9]: The system must implement some form of accurate access control on databases.

### 3.3.1 Visitor Use Case Diagram




### 3.3.2 User Use Case Diagram

### 3.3.3 Third Party Use Case Diagram

### 3.3.4 System Manager Use Case Diagram ???

???????

## 3.4 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.

## 3.5 Desgin Constraints

### 3.5.1 Standards Compliance

### 3.5.2 Hardware Limitations

### 3.5.3 Other Constraints

## 3.6 Software System Attributes

### 3.6.1 Reliability

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

### 3.6.2 Availability

The system must fullfil 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 redudant in different servers. In this way, the malfuction of a service will not cause a service breakdown, but only a decrease of performance.

### 3.6.3 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.

### 3.6.4 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.

### 3.6.5 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 assumptioms | 2 |
| 22/10/2018 | UML and Non-Functional Requirements | 3.5 |
| 25/10/2018 | Functional Requirements | 3 |
| 26/10/2018 | Statechart Diagrams | 2 |
| Total | | 13 |

- 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 |
| Total | | 11.5 |

# 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