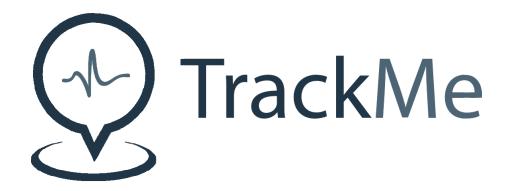**POLITECNICO**
MILANO 1863

Computer Science and Engineering
Software Engineering 2 Project

TrackMe

Requirement Analysis and Specification Document

Gargano Jacopo Pio, Giannetti Cristian, Haag Federico

Anno Accademico 2018-2019

Contents

Chapter 1

Introduction

1.1 Purpose

TrackMe wants to offer a service named "Data4Help" on top of which will be built two services named "AutomatedSOS" and "Track4Run".

Data4Help: the basic idea behind Data4Help is to acquire the location and health data of *Users* through *Smart wearables* connected to a smartphone. Moreover, data can be directly sent to *Third Party* customers who pay for the service. In order to analyze *Users data*, these need to obtain *User* authorization. Furthermore, they can request anonymized data of a group of *Users*.

AutomatedSOS: a service offered only to subscribed customers that constantly monitors their health status. Its purpose is to identify when a *User* is in need of immediate assistance and send an ambulance to their location.

Track4Run: a service used to track runners participating in running competitions. *Organizers* will be able to define a path for the run, *Participants* will share their position and health data and *Spectators* may watch the competition on their smart devices.

1.2 Scope

TrackMe offers its services in a world where technology and health are taking huge strides forward every day and innovation is commonplace.
Nowadays, people use smart devices such as smartphones and smart wearables more than any other object that they own. This means that any activity they perform already is or can be integrated with these devices.
TrackMe, with the introduction of Data4Help, offers the possibility to monitor users' location and health data and allows third parties to register in the system

to acquire these data.

When it comes to personal data acquisition, privacy is a fundamental issue that TrackMe needs to consider. Privacy is, in fact, regulated by several laws: there are many restrictions on how user's data is acquired and stored. Therefore, TrackMe is concerned with users' consent to transferring data to TrackMe itself and to third parties for individual specific analysis. Moreover, TrackMe guarantees that anonymized data of groups of individuals are properly anonymized by checking specific constraints.

Over the course of their daily routine, users perform several actions during which their data can be analyzed to provide them with insights. For instance, they might want to monitor their heart rate while sleeping or to keep track of the distance they have walked during their day and the places they have been to.

People with a potential need for immediate assistance have always been a huge concern for their relatives and for technology makers. These may include old people with limited movement and a high chance to need urgent assistance, anyone who has a specific disease, but also a healthy individual who can suffer from a sudden heart failure. Until now, the only practical way to receive help has been to call for help, either by using a cell phone or by pushing an SOS button on a dedicated device. TrackMe proposes to automatize the step of calling for help through AutomatedSOS. In fact, when determined health values will no more be considered as normal, the system will automatically send a request for help.

Another part of the market that TrackMe decided to enter, is the sport one, where having the possibility of collecting and sharing data about people is nowadays disruptive.
A sport practiced and loved by many is running. Organizing a run requires several steps to be taken such as defining a path, getting athletes to participate and spectators to watch it. TrackMe proposes to simplify the organization of a run, by introducing Track4Run. This service will allow the definition of a path, easy enrollment for participants and a real-time tracking of each runner's position on a map.

1.2.1   Analysis of shared phenomena

TO DO LIST OF SHARED PHENOMENA

1. users move (or run in Track4Run)

2. users can have health problems

3. sensors collect data

4. sensors communication

5. sensors break

6. third parties collect data from the system

7. third parties registration to Data4Help

8. user grant direct usage of personal data

9. user registration (Data4Help and/or services built on top of it)

10. organizers of run define path

11. participants of run enroll to it

12. run spectators see on a map the position of runners

1.3 Goals

1.3.1 Data4Help

G_1 Collect *User data* through *smart wearables*.

G_2 Send specific *User data* to *Third parties* only if *User* consent was given after *Third party* access request.

G_3 Send requested *Group data* to *Third parties* if the group it refers to is made up of 1000 or more Users.

G_4 Send *Users data* and *Group Data* to subscribed authorized *Third parties* as soon as they are produced.

G_5 Allow *Users* to subscribe to *Services*.

1.3.2 AutomatedSOS

G_6 Analyze *User data* to check whether or not a *User* is as a *User in need*.

G_7 Send an ambulance to the last position of a *User in need*.

1.3.3 Track4Run

G_8 Allow *Organizers* to create a *Run*, defining a path.

G_9 Allow *Users* to enroll in a *Run* as *Participants*.

G_{10} Allow *Spectators* to watch a *Run*.

1.4   Definitions, Acronyms, Abbreviations

1.4.1   Definitions

User : registered individual of Data4Help who agreed on the acquisition and processing of their data (see add reference to user data below).

User data : *User*'s health data and location acquired by Data4Help

Third party : a company that can access *User data* stored in TrackMe's database, after user consent.

Service : application available for some Data4Help *Users*, generally offered by a Third party.

Organizer : companies or private persons organizing running competitions.

Spectator : people participating as spectators to running competitions.

Participant : people running in running competitions.

Group data : group of *Users data* acquired by Data4Help.

Smart wearable : smart devices that can be worn on the body as accessories. These devices are required to have specific sensors for data acquisition, to be compatible with the system to be (see add reference to requirements for smart wearables). The adjective 'smart' refers to the possibility of connecting them to an external device, such as a smartphone, and to the ability of operating autonomously even if not connected.

Anomalous data : health data that is outside certain intervals, which identify a *User* normal health condition. define better

User in need : registered user of AutomatedSOS in need of assistance since their health data is *amomalous*.

1.4.2   Acronyms

GPS : Global Positioning Service

1.4.3   Abbreviations

G$_n$: nth goal

D$_n$: nth domain assumption

R$_n$: nth requirement

1.5   Revision history

1. v. 1.0

1.6   Reference Documents

TO DO DURING THE WRITING OF THIS DOCUMENT

1.7   Document Structure

WORK IN PROGRESS

Chapter 2

Overall Description

2.1 Product perspective

Class Diagram

Data4Help

- User subscribes to Data4Help

- User log in to Data4Help account on the app

- User adds a new service on personal Data4Help account granting to it the direct access of data

- User unsubscribes from Data4Help

- Smart wearables send data to Data4Help system

AutomatedSOS The product, because it is built on top of Data4Help, inherites from it the same shared phenomena.

- User becomes a User in need

- The system calls an ambulance

Track4Run The product, because it is built on top of Data4Help, inherites from it the same shared phenomena.

- Organizer sets a path for a running competition

- User enrolls to a running competition

- Spectator watches the participants' tracking map

2.2   Product functions

2.2.1   Data4Help

User Registration

Data4Help will allow individuals to register. These will register by entering all the required information (see [R$_\text{X}$] add reference to Requirements where we specify User info for registration). When registering to Data4Help, an individual will first declare to have read the privacy statement and secondly they will have to accept the terms and conditions, which specifically include their consent to the acquisition and processing of their data, including sensitive ones, by TrackMe.
The user registration process will be carried out on the user dedicated application (see add reference to where we are going to specify the user interface - probably section User Interface (mobile app), maybe add also reference to user registration scenario / use case.
Unregistered *Users* will not be able to use Data4Help. (maybe this is a requirement and it is not necessary to put it here)

Third Party Registration

A *Third Party* may register to Data4Help through the *Third Party* dedicated form (seereference), including all required information (see [R$_\text{X}$] add reference to Requirements where we specify *Third Party* info for registration). Once a terms and conditions have been agreed accepted by the *Third Party*, it will be successfully registered to the service.
Third Party registration is required for using the service: an unregistered *Third Party* must not be able to access *Users data.*(maybe this is a requirement and it is not necessary to put it here).

User Data Acquisition

Data4Help will acquire *Users data* through *Smart wearables.*
Users must give consent to the acquisition of their data when registering to

Data4Help.

Data acquisition frequency can be changed according to *Users* or *Third Parties* needs. For instance, if a *User* wants to save their *Smart wearable* battery, frequency can be reduced. On the other hand, if a *Third Party* would like to track more accurately the position of a *User*, a higher location acquisition frequency can be requested.

Third Parties Data Access

Once a *Third Party* is registered to Data4Help, it can request access to *Users data* acquired through Data4Help and stored by TrackMe. *Third Parties* may request data that refers either to a specific individual - *User data* - or to a group of *Users* - *Group data*.

Consent to individual data access is left to the specific *User*, who can either allow or deny a *Third Party* request.

Group data will be shared with *Third Parties* as long as TrackMe will be able to anonymize it properly (see R$_X$ include reference to requirement about anonymized data (1000 users satisfy request).

Data Management and Privacy

All data acquired through Data4Help will be stored on a database accessible only by TrackMe. Each piece of *Users data* will have a list of *Third Parties* to whom access was granted. At any time, a *User* will be able to revoke the previously given consent to any *Third Party* or to TrackMe. Moreover, a *User* may exercise their right to data portability, which means that TrackMe will have to provide them with all the collected data regarding them. Finally, *Users* may ask the deletion of all their data stored by TrackMe. might want to list the requirements that relate to this

By guaranteeing these functions, Data4Help will respect existing general regulations on privacy (e.g. EU GDPR).

2.2.2   AutomatedSOS

User Subscription

All Data4Help *Users* may subscribe to AutomatedSOS through Data4Help application(see add reference).

Health Status Monitoring

The service will constantly monitor *User*'s health data to verify if it is *Anomalous*. While data acquisition frequency can be tweaked only by Data4Help, AutomatedSOS may request a different value according to user needs. check this: When the service is not receiving data, it may try to contact the *User*. Otherwise, it may send an alert to a close friend of the *User* for them to check in.

Calling an Ambulance

check this title In case the health status of a subscribed *User* is considered not to be good, AutomatedSOS will make a call to local emergency services within 5 seconds and send an ambulance to the last registered location of the *User*.

2.2.3   Track4Run

User Registration

Track4Run will be a service used by three different kinds of *Users*: *Organizers*, runners and *Spectators.Organizers* will register to Track4Run by filling in all required information in the organizers registration form (see include ref to requirements for organizers registration). *Participants* will enroll in the run using their Data4Help credentials through the Data4Help application. *Spectators* will just need to know the *Run identifier* and entering when requested where??.

Run Creation and Path Definition

Organizers have the ability of creating a run. They will be able to give the run a name, set a date and time the run is going to be held on and define a path for it. Premium functions will be included in Track4Run. One of them will be sending an invitation to specific *Participants* via email. Another premium function will allow *Organizers* to make their run public and let anybody enroll to it or be a *Spectator* of it. Finally premium *Users* will be able to put constraints to specific parameters of the runners, including but not limited to age, sex and weight.

Runners Map Display

Track4Run will display a map with the real time position of all the *Participants*. add info

2.3   User characteristics

2.3.1   Data4Help

Users: People having at least one device with a sensor connected to internet, willing to share the collected data with TrackMe to take advantage of the company rewards and eventually use the services built on top of Data4Help service.

Third parties: Companies or private persons willing, for any reasons, to collect bulk data. Usually the data is used for building services on top of it; in this case it is very important that data is transferred real time. Sometimes it is used just for statistics analysis. In both cases, *Third Parties* need that the data is correct and precise.

2.3.2 AutomatedSOS

Users: People (mainly elderly) having some disease or high risk of disorder willing to monitor own health parameters and conditions in order to prevent and possibly avoid crisis.

2.3.3 Track4Run

Participants: People participating in running competition. Need to have small device and with no interaction during the run to avoid distractions.

Organizers: Companies or private persons organizing running competitions willing to better engage the spectators giving the possibility to track in real-time the position of all participants. Need to provide the service easily to ensure *Spectators* are not prevented in using it.

Spectators: People participating as *Spectators* to running competitions, willing to better engage the event by tracking the runners during all the run. Want it to be easy without needed particular devices or applications. Usually it is a "one-time usage".

2.4 Assumptions, Dependencies and Constraints

2.4.1 Domain Assumptions

D_1 Personal data inserted by the *User* during the registration correspond to his real data

D_2 Data collected and sent by the GPS and the sensors at a certain instant correspond to the status of the *User* at that time

D_3 *User* is logged in one device at a time

D_4 The maps used faithfully represent the streets that can be traveled

D_5 *Third Party* can receive granting for direct data access only trough a service and can use that data only for that service.

WORK IN PROGRESS

Chapter 3

Specific Requirements

3.1 External Interface Requirements

3.1.1 User Interfaces

WORK IN PROGRESS

3.1.2 Hardware Interfaces

WORK IN PROGRESS

3.1.3 Software Interfaces

WORK IN PROGRESS

3.1.4 Communication Interfaces

WORK IN PROGRESS

3.2 Functional Requirements

3.2.1 Scenarios

3.2.2 Use Cases

Data4Help

Name	User Sign Up
Actors	*User*, Data4Help
Entry Conditions	*User* successfully installed Data4Help application on their smartphone.

Events Flow	
	1. *User* taps on "Sign Up" button.
	2. *User* fills in all required fields for *User* registration.
	3. *User* taps on "Create an Account" button.
	4. Data4Help saves *User* information.
Exit Condition	*User* successfully registered by Data4Help.
Exceptions	
	1. Inserted email already registered for another *User*.
	2. Inserted password is not valid.
	3. Not all required fields are filled in.
	4. *User* already signed up.
	User is invited to try again.

Name	Third Party Sign Up
Actors	*Third party*, Data4Help
Entry Conditions	*Third party* is connected to the *Third party* dedicated website (see add reference).
Events Flow	
	1. *Third party* clicks on "Sign Up" button.
	2. *Third party* fills in all required fields for *Third party* registration.
	3. *Third party* clicks on "Create an Account" button.
	4. Data4Help saves *Third party* information.
Exit Condition	*Third party* successfully registered by Data4Help.

Exceptions	
	1. Inserted email already registered for another *Third party*.
	2. Inserted password is not valid.
	3. Not all required fields are filled in.
	4. *Third party* already signed up.
	Third party is invited to try again.

Name	User Log In
Actors	*User*, Data4Help
Entry Conditions	*User* successfully registered to Data4Help and installed Data4Help application on their smartphone.
Events Flow	1. *User* enters username.
	2. *User* enters password.
	3. *User* taps on "Log In" button.
	4. Data4Help checks *User* credentials.
Exit Condition	*User* is successfully logged in.
Exceptions	1. Inserted username is not valid.
	2. Inserted password is not correct.
	User is invited to try again.

Name	Third Party Log In
Actors	*Third party*, Data4Help
Entry Conditions	*Third party* successfully registered to Data4Help and is connected to the *Third party* dedicated website (see add reference).

Events Flow	
	1. *Third party* enters username.
	2. *Third party* enters password.
	3. *Third party* clicks on "Log In" button.
	4. Data4Help checks *Third party* credentials.
Exit Condition	*Third party* is successfully logged in.
Exceptions	
	1. Inserted username is not valid.
	2. Inserted password is not correct.
	Third party is invited to try again.

Name	Third Party requests User Data
Actors	*Third party*, Data4Help, *User*
Entry Conditions	*Third party* and *User* successfully registered to Data4Help.
Events Flow	
	1. *Third party* requests access to specific *User data*.
	2. Data4Help forwards the request to the specific *User*.
	3. *User* gives consent to the requesting *Third party* to access their data, unless already given.
Exit Condition	Data4Help sends *User data* to the *Third party*.
Exceptions	
	1. *User* denies consent to their data access by the requesting *Third party*.

Name	Third Party requests Group Data
Actors	*Third party*, Data4Help
Entry Conditions	*Third party* successfully registered to Data4Help.

Events Flow	
	1. *Third party* requests access to *Group data*.
	2. Data4Help checks if the requested data refers to minimum 1000 *Users*.
Exit Condition	Data4Help sends *Group data* to the *Third party*.
Exceptions	
	1. *Group data* refers to less than 1000 *Users*.
	Data4Help denies *Group data* access to the *Third Party*.

? ? ? Collect data –¿ probably it is not a use case, but regular product function Third party subscribes to data User revokes consent ? ? ? User manages data (gdpr)

AutomatedSOS

3.3 Performance Requirements

WORK IN PROGRESS

3.4 Design Constraints

3.4.1 Standards compliance

WORK IN PROGRESS

3.4.2 Hardware limitations

WORK IN PROGRESS

3.4.3 Any other constraint

WORK IN PROGRESS

3.5 Software System Attributes

3.5.1 Reliability

WORK IN PROGRESS

3.5.2 Availability

WORK IN PROGRESS

3.5.3 Security

WORK IN PROGRESS

3.5.4 Maintainability

WORK IN PROGRESS

3.5.5 Portability

WORK IN PROGRESS

Chapter 4

Formal Analysis using Alloy

WORK IN PROGRESS

Chapter 5

Effort Spent

WORK IN PROGRESS

Chapter 6

References

WORK IN PROGRESS