Politecnico di Milano

Master's Degree in
Computer Science and Engineering

Software Engineering 2

TrackMe
Requirements Analysis and Specification Document

Authors
Alberto Archetti
Fabio Carminati

Reference professor
Elisabetta Di Nitto

v.0.0 - October 23, 2018

Contents

1 Introduction

1.1 Purpose

This is the Requirement Analysis and Specification Document (RASD) of `Data4Help` and `AutomatedSOS` services, commissioned by TrackMe company. We will specify goals, domain assumptions, requirements, interfaces and high-level models using `UML` and `Alloy` languages of the systems that will be produced. This is an important step in software development, because identifying from the starts the correct scope, the constraints and the overall structure of our products is the key to produce mantainable and secure software that correctly responds to the stakeholder's needs.
The audience of this document is very wide. It includes

- stakeholders, as it acts as a contract that certifies what is required to our final product in order to satisfy their needs
- developers that will be guided by this document's prescriptions
- testers that are asked to verify the correspondence between the implementation and the requirements
- managers, in order to keep track of the project development

Requirement analysis and elicitation is an iterative process. This is the version `v.0.0` of the RASD document. See section 1.4 for more details on revision history.

1.2 Scope

1.2.1 Project description

TrackMe wants to develop a software-based service that allows individual users to collect health data, called `Data4Help`. This data, stored in the `Data4Help` system, can be retrived and visualized according to different filters and projections.
The system allows third parties registration. Third parties can request access to users'collected data in two ways:

Single-person data After the request by the third party is made through the system interface, the system asks the user for authorization; if positively provided, the third party is granted access to the user's data

Amonymous-group data Thirs parties can be interested in big amounts of data, regarding who are the people that are providing it; the system, once the request by the third party is sent, checks if the data can be effectively anonymized (it must find at least 1000 people that match the third party request) and, if positively evaluated, grants access to the anonymized data to the third party that requested it

Third parties can subscribe to new data and receive it as soon as it is collected by the system.

Another service that TrackMe wants to develop is `AutomatedSOS`, built on `Data4Help`. This service analyzes users'data and calls a SOS whenever data exceedes the basic health parameters. For this particular purpose, system performances will be a critical aspect to be taken into account, because even the slightest delay matters in critical health situations.

1.2.2 Goals

Here we present the goals that will be reached once the project is completed. Goals with identifier that starts with `G.U` focus on the users, while goals with identifier that starts with `G.T` focus on third parties.

`G.U1` Users can

- `G.U1.1` collect[1] their health data
- `G.U1.2` store[2] their health data
- `G.U1.3` manage[3] their health data

`G.U2` Users can decide which data can be anonymously shared to third parties

`G.U3` Users can decide whether to accept or decline third paties'requests for their data sharing

`G.U4` Users can revoke the data sharing permissions for both anonymized data (see `G.U2`) and single-user data (see `G.U3`); once the permission is revoked, the third party will still have access to the previously acquired

[1] acquire data through external devices

[2] data shouldn't be lost once acquired and should be always retrievable by the user that produced it and by third parties that have access to it

[3] search through data by time intervals and filter data by type

data of the user, but will not have access to newly produced data by the user that fits the revoked request[4]

`G.U5` If a user chose to be monitored by `AutomatedSOS` system and his/her health parameters are critical, then an ambulance will be dispatched within 5 seconds and then arrive at the user's location

`G.T1` Third parties can ask to a user the permission for sharing some[5] of his/her data; if the user accepts the request, his/her data that fits the request is then accessible by the third party, otherwise the data is not not accessible by the third party

`G.T2` Third parties can request access to anonymized data of a group of individuals; if the data can be anonymized, then the third party that made the request gains access to the data, otherwise it has no access to it; the shared data should be properly anonymized (the third party shouldn't be able to discover who are the users that produced that data)

`G.T3` Third parties can revoke their data requests; they still have access to the previously acquired data, but will not receive any more data that fits the revoked request

1.3 Definitions, acronyms, abbreviations

1.3.1 Definitions

(To have) access to the data A user has access to the data if he produced it i.e. if the data was while logged in the user's profile; a third party has access to the data if retrived by the system through external sensors

Anonymized data Data is said to be anonymized if it has no information about the user that produced it; a set of data (also known as aggregate data or group of data) is said to be anonymized if it contains only

[4]data is said to *fit the revoked request* if 1. it would be shared if the request is accepted but not revoked 2. it would not be shared if the request has been accepted, then revoked; see Section 1.3.1 for more details

[5]data can be requested by third parties according to the `Package` concept; see Section 1.3.1 for more details

anonymized data and its cardinality (number of elements contained in it) is greater or equal to 1000

Data Information about health parameters that has been retrived by the S2B through sensors while logged in a user profile; data belongs to that user and he/she can retrive it from the system; data tuples are identified by the owner user and the acquisition timestamp

Data fits the request Data is said to fit a particular request if the following holds:
1. if the request is accepted but not revoked by the target user, then it would be shared between the user and the third party that made the request
2. if the request has been accepted and after revoked by the user, then it would not be shared between the user and the third party i.e. the third party cannot retrive the data it asked

Health parameter Numerical variable that encodes information about a physical phenomena that can be related to the person's health and can be measured through external sensors

`Package`

Request Making a request means asking for a permission to access some data; a request is made by a third party and the target can be a single user's data (the third party wants to have access to the user's data) or aggregate data (the third party is interested in a huge number of data that has been anonymized by the system); a request can be accepted (third party gains access to the data that fits the request) or declined (third party has no access to that data)

Threshold Health parameters, as numerical variables, can be labled as *ordinary* or *critical* according to some intervals; these intervals are defined through thresholds that separate the *ordinary* domain to the *critical* one; thresholds are a domain property

Timestamp A timestamp[6] is a sequence of characters or encoded information identifying when a certain event occurred, usually giving date and time of day, sometimes accurate to a small fraction of a second

[6] `https://en.wikipedia.org/wiki/Timestamp`

1.3.2 Acronyms

1.3.3 Abbreviations

S2B

1.4 Revision history

Version	Log
`v.0.0`	Introduction sketch

1.5 Reference documents

See References for details on the consulted documents.

1.6 Document structure

This document uses the IEEE standards for requirement analysis documents as a guideline towards a clear and logical explanation of its contents:

- Section 1 gives a brief introduction on the project to be developed and adds notes on references and revisions
- Section 2 describes the world and the shared phenomena, by defining assumptions and constraints; it identifies also the goals and the main functions of the project
- Section 3, as the main part of this document, is about requirement analysis; it has also sections about interfaces of the system and software attributes
- Section 4 contains the `Alloy` model that certifies correctness of goals implication by requirements and domain assumptions
- Section 5 lists the overall modifications and additions to this document, ordered by date, as the hour counter of effort spent by each group member

2 Overall description

2.1 Product perspective

2.2 Product functions

2.3 User characteristics

2.3.1 Actors

User Person that has successfully created an account of TrackMe. She or He can exploit all the functionalities of the application

Third Party Entity that can request to Data4Help the access to either individual or group DataSets

2.4 Assumptions, dependencies, constraints

2.4.1 Domain assumptions

`D1` da 1

`D2` da 2

3 Specific requirements

3.1 Scenarios:

3.2 External interface requirements

3.2.1 User interfaces

3.2.2 Hardware interfaces

3.2.3 Software interfaces

3.2.4 Communication interfaces

3.3 Functional requirements

3.4 Performance requirements

3.5 Design constraints

3.5.1 Standards compliance

3.5.2 Hardware limitations

3.5.3 Any other constraint

3.6 Software system attributes

3.6.1 Reliability

3.6.2 Availability

3.6.3 Security

3.6.4 Mantainability

3.6.5 Portability

4 Formal analysis using Alloy

5 Effort spent

References

[1] Mandatory Project Assignment AY 2018-2019

[2] IEEE 830-1993 - IEEE Recommended Practice for Software Requirements Specifications

[3] ISO/IEC/IEEE 29148 - Systems and software engineering — Life cycle processes — Requirements engineering

[4] Collection and Processing of Data from Wrist Wearable Devices in Heterogeneous and Multiple-User Scenarios
`https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5038811/`

[5] Google Fit API
`https://developers.google.com/fit/overview`

[6] Slides of the course by Prof. Di Nitto
`https://beep.metid.polimi.it/`

[7] LaTeXtemplates
`http://www.latextemplates.com/`
`http://www.overleaf.com/latex/examples/title-page-with-logo/hrskypjpkrpd`