



POLITECNICO

MILANO 1863

Software Engineering 2

Design Document

Work team:

Paolo Romeo, Andrea Scotti, Francesco Staccone

AY 2018-2019

Table of contents

1. Introduction
 - 1.1. Purpose
 - 1.2. Scope
 - 1.3. Definitions, acronyms, abbreviations
 - 1.4. Revision history
 - 1.5. Reference documents
 - 1.6. Document structure
2. Architectural design
 - 2.1. Overview:High-level components and their interaction
 - 2.2. Component view
 - 2.3. Deployment view
 - 2.4. Runtime view
 - 2.4.1. Sign up Runtime View
 - 2.4.2. Login Runtime View
 - 2.4.3. Join a run Runtime View
 - 2.4.4. Organise a run Runtime View
 - 2.4.5. Individual request Runtime View
 - 2.4.6. Group request Runtime View
 - 2.5. Component interfaces
 - 2.5.1. REST API
 - 2.6. Selected architectural styles and patterns
3. User interface design
 - 3.1. UX Diagram
4. Requirements traceability
5. Implementation, integration and test plan
6. Effort spent
7. References

1. **Introduction**

1.1. *Purpose*

This document is thought to be an overview of the TrackMe application, in which is explained how to satisfy the several project requirements stated in the RASD. This document is principally intended for the developers and the testers, with the purpose of providing a functional description of the main architectural components, their interfaces and their interactions, along with the design patterns.

1.2. *Scope*

—Presentation—

TrackMe is structured in a multi-tier architecture. More specifically, the Business logic layer has the task of taking charge of the incoming requests/data, computing checks, and interacting with external third-party services through the use of interfaces. This layer is connected with the Data layer, in which are stored all the Users data (credentials, health data). The Presentation layer is build through the fat Client paradigm in which the client needs to perform computation to temporarily store health data in the local memory in case of missing internet connection between the client and the server.

1.3. *Definitions, acronyms, abbreviations*

1.3.1. **Definitions**

- User: a registered individual who can use the TrackMe services.
- Third party: a registered entity that can use the TrackMe services.
- Client: A client is a piece of computer hardware or software that accesses a service made available by a server;
- Firewall: A network security system that monitors and controls incoming and outgoing network traffic based on predetermined security rules;
- Server: A computer program or a device that provides functionality for other programs or devices, called "clients".

1.3.2. **Acronyms**

- API: Application Program Interface;
- DBMS: Database Management System;
- DD: Design Document
- GUI: Graphical User Interface;
- HTTP: Hypet Text Transfer Protocol;
- MVC: Model View Controller pattern;
- OS: Operating System;
- RASD: Requirements Analysis and Specifications Document;
- REST: REpresentational State Transfer;

1.3.3. **Abbreviations**

- Gn: n-goal in the RASD;
- Rn: n-functional requirement in the RASD;

1.4. *Revision history*

- 10/12/2018 Version 1.0

1.5. *Reference documents*

- RASD document;
- Mandatory project assignment;

1.6. *Document structure*

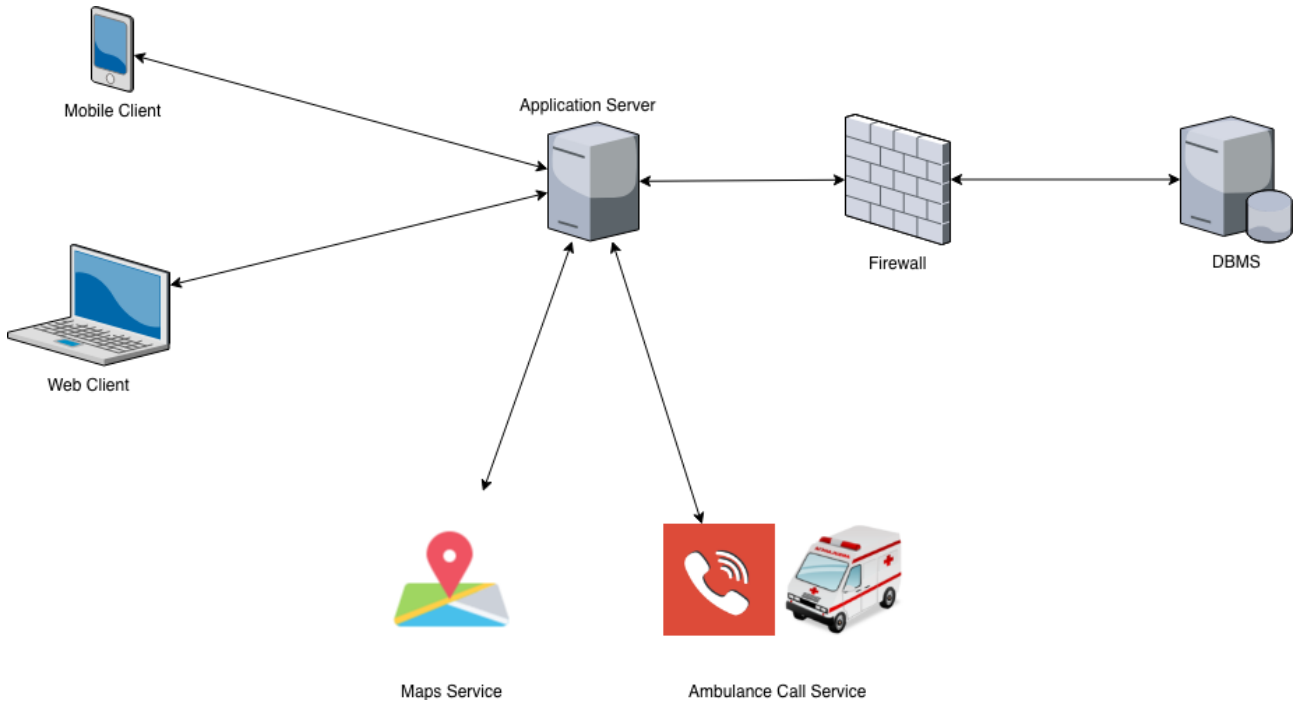
The following document is organised in this way:

- Architectural Design: this section shows the main components of the system and the connections among them. It will also focus on design choices, styles and patterns.
- User Interface Design: this section includes an improvement of the user interface given in the RASD document. It will be described through the use of UX modeling.
- Requirements Traceability: this section shows how the requirements in the RASD are mapped to the design components presented in the DD;
- Implementation, Integration and Test plan: this section shows the order in which the implementation and the integration of the subcomponents will occur and how the integration will be tested.

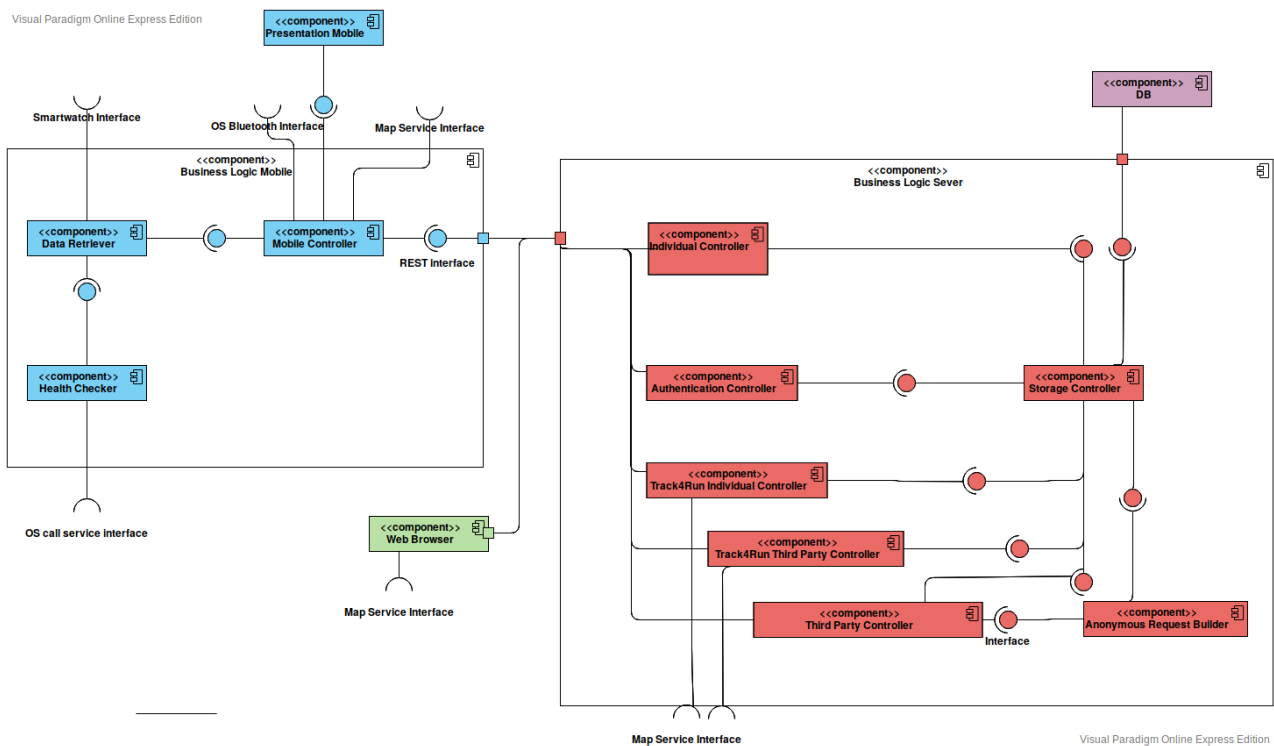
2. Architectural design

2.1. Overview: high-level components and their interaction

The figure below represents an high level overview of the system. Further details on the system components and their interaction will be further explained in the next sections.



2.2. Component view



The UML component diagram shows the internal structure of the system highlighting the individual

modules and the connections among them. It models the static implementation view of a system by breaking it down into various high levels of functionality. Individual components are wired together by using an assembly connector to connect the required interface of one component with the provided interface of another component. For simplicity reasons, the interfaces between REST controllers (Individual, Third Party, Track4Run Individual and Track4Run Third Party Controller) and the Authentication Controller have not been drawn in the diagram. However they are present in the system in order to validate the successive user sessions after the log in. Below is the description of the components:

- **Mobile Controller**

This is the component that allows the individual mobile application to access to the API of the Business Logic Server. It implements the interface dedicated to the transfer of data from client to server and it translates the individual user interactions in REST API calls. If internet connection is not available or it's too slow, older health and location data are not saved locally but discarded by giving priority to new data.

- **Data Retriever**

This component retrieves health data from smartwatches or similar devices, it filters them and forwards them to the Health Checker component, if the AutomatedSOS service is enabled, and to the Mobile Controller component.

- **Health Checker**

This component analyzes in real time health data of the individual and checks if his or her health is fine. If it's not it interact with the operating system of the running application in order to make a SOS call.

- **Presentation**

This is the component that is aimed to display the front-end content to the individual and to allow him or her to interact with the application.

- **Web Browser**

The system allows the third party to interact with it through any web browser.

- **Individual Controller**

The main role of this component is to manage the data coming from the specific individual by invoking the proper methods of the Storage Controller. It also provides methods to accept/refuse a request of agreement and to change personal information or preferences. Furthermore it notify to the client if there are new requests or info for him.

- **Third Party Controller**

This component provides methods that allow the third party to send individual and anonymous requests to the system. If there are new individual agreements or new data available, it sends them to the third party.

- **Authentication Controller**

This component provides authentication and registration processes for both the individuals and the third parties.

- **Track4Run Individual Controller**

This component provides the methods to permit an individual to join, leave, check and watch a run. It communicates with the external service that provides maps through the Map services interface. Every time a user wants to join a run, it checks if all the constraints are satisfied. Finally, it keeps updated the individual about new info by sending him or her notifications.

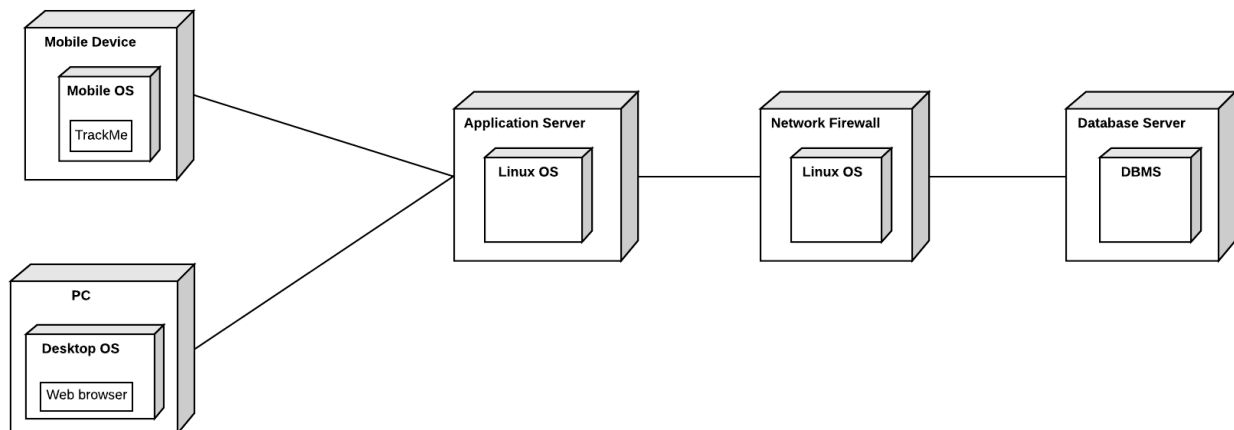
- **Track4Run Third Party Controller**

This component provides the methods to allow a third party to organize a run. It communicates with the external service that provides maps through the Map services interface to allow the third party to select the track for the run.

- **Storage Controller** This component provides the methods for querying and updating the Database.
- **Anonymous Request Builder** This component aggregates data in order to answer to third party group requests by assuring anonymity.
- **Database** This component represent the DBMS. It provides the interfaces to retrieve and store data. In the database there are data about users, third parties and the set of agreements among them. It also contains data about the runs.
- **External services interfaces**
These interfaces are not implemented by the system but are provided by external services in order to run the application.
 - **Map Service Interface**
It allows the third party to select the track and to show the position of runners in real time on the map.
 - **OS Call Service Interface**
It allows the mobile application to make a SOS phone call in case of emergency.
 - **OS Bluetooth Interface**
It allows the mobile application to connect the smartphone to smartwatches or similar devices.
 - **Smartwatch Interface**
It allows the mobile application to get data from smartwatches.

2.3. Deployment view

The figure below shows the deployment diagram of the whole system. Its main goal is to describe the distribution of components capturing the topology of the system's hardware.



As previously stated in the section 1, the system is structured in a multi-tier architecture. The specific role of each node is clarified here:

Clients

The first tier is composed by the clients machines (mobile for individuals and desktop for third parties). The individuals will be able to access TrackMe functionalities through the dedicated native application while the third parties through any web browser.

Application Server

This is the middleware level of the architecture: all the business logic of the system is contained in this server.

Network Firewall

The access to the Database is mediated by a network firewall in order to avoid unauthorised access to the data and the credentials of the user.

Database Server

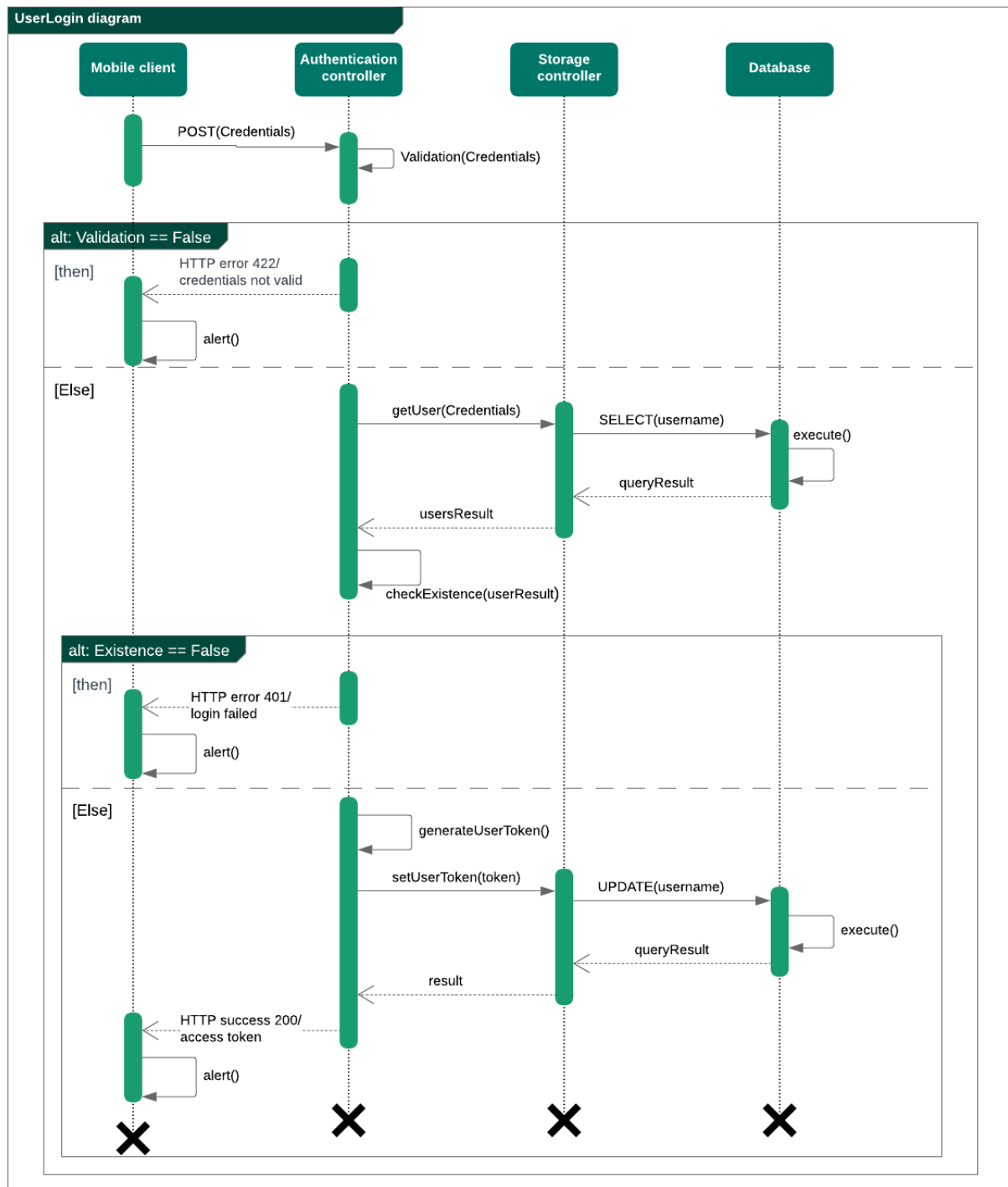
This is the last layer of the architecture: all the data are stored in a Database Server accessed through a relational DBMS.

2.4. *Runtime view***2.4.1. Sign up Runtime View**

Third parties and individuals have to sign up to the application before being able to access its functionalities. The registration process is the same for both third parties and individuals, the only thing that differentiates it is the information provided by them. The third party must fill up a form with its VAT number and a password. To reach the same goal an individual must fill up a form with username, password and personal data. The information is serialized and then sent to the Application Server through an HTTP POST request. The Authorization controller handles the request and, through the Storage interface, creates a new entry in the User table or in the ThirdParty table on the Database.

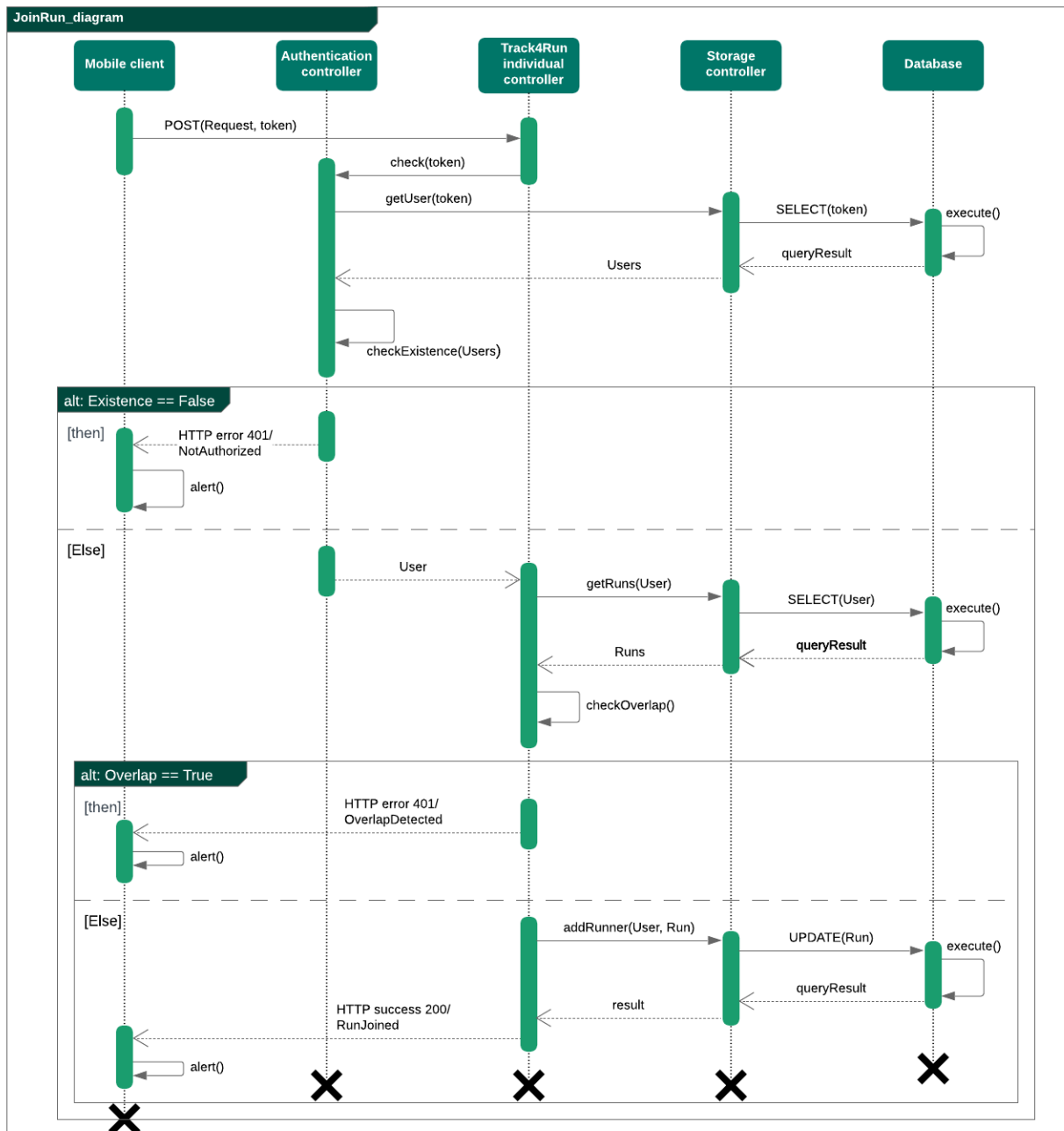
2.4.2. User Login Runtime View

Third parties and individuals have to be logged to the application before being able to access its functionalities. Both third parties and users submit the login information through and HTTP POST request. The request is handled by the Authentication Controller that validates the request and checks if the Database has an entry for the requested account. If the entity is present and the credentials are correct, the Authentication Controller generates an Access Token, sets it as the current access Token for the specified entity and returns it to the entity itself. The following sequence diagram shows how the process works in detail for the login of an individual user.



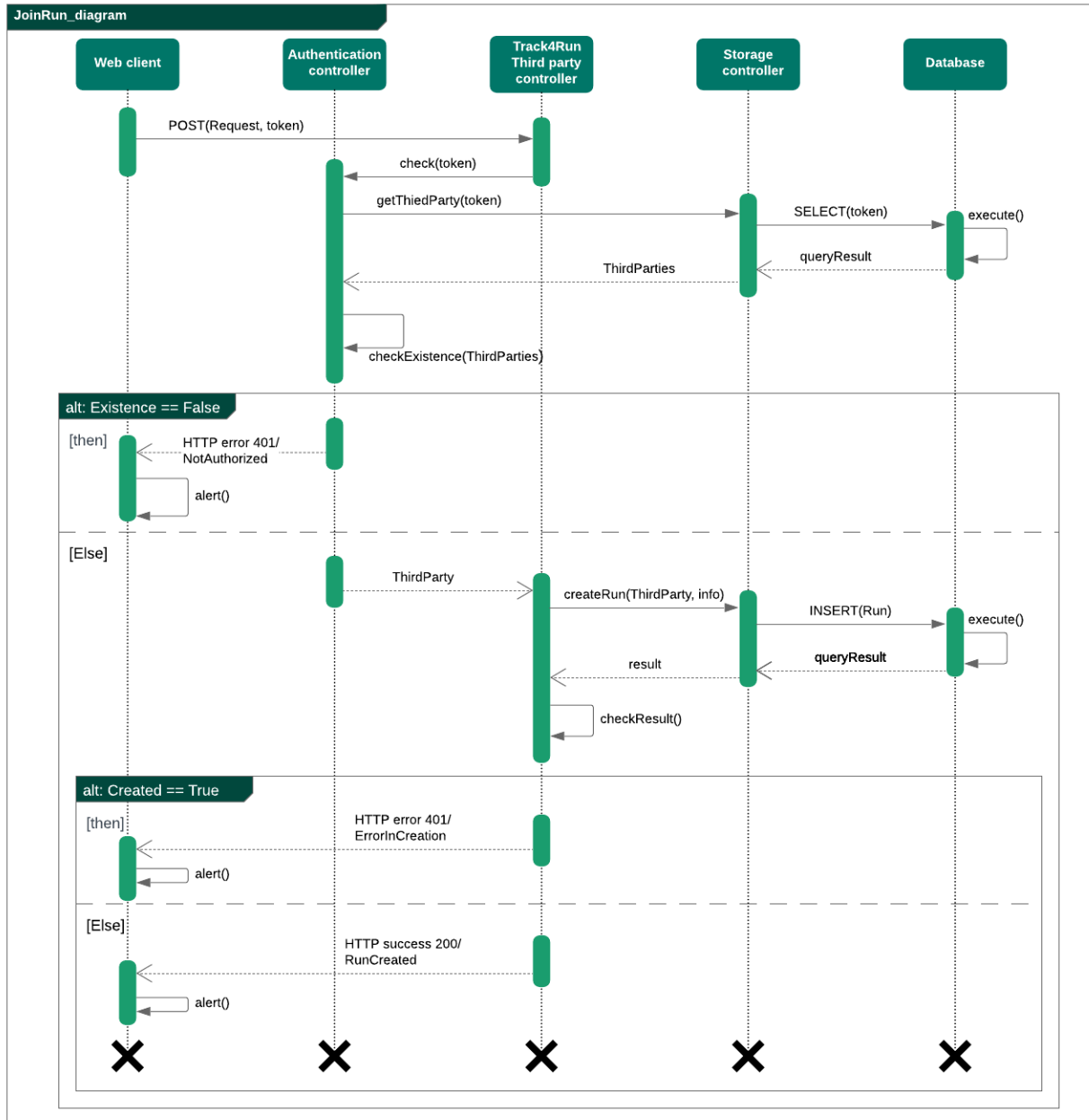
2.4.3. Join a run Runtime View

The User opens the Track4Run section of the application and, after a GET request to the Application Server he/she receives the list of all the available runs and he/she can choose to join one of them (if there is at least one displayed run). The User can send a POST request containing the Access Token and the selected run to the Track4Run Individual Controller. The Track4Run Individual Controller passes the Access Token to the Authentication Controller that checks if the Mobile Client provided a valid Token. If the Authentication succeeds the control goes back to the Track4Run Individual Controller that checks if the user has already joined an overlapping run or if the maximum number of participants was reached. If the control is satisfied the Track4Run Individual Controller asks the Storage Controller to update the tuple of the selected run in the Database. To avoid repetitions, the following sequence diagram shows the process assuming that the User already received the list of available runs.



2.4.4. Organise a run Runtime View

The Third party opens the Track4Run section of the application and, after filling the form containing the information about the run it can send a POST request containing the Access Token and the filled form to the Track4Run Third Party Controller. The Track4Run Third Party Controller passes the Access Token to the Authentication Controller that checks if the Web Client provided a valid Token. If the Authentication succeeds the control goes back to the Track4Run Third Party Controller that asks the Storage Controller to insert a new tuple for the run in the Database.



2.4.5. Individual request Runtime View

2.4.6. Group request Runtime View

2.5. *Component interfaces*

- **Authentication Controller**

Third Party Registration

endpoint	*/auth/thirdparty/register
method	POST
url params	
data params	VAT: [alphanumeric] password : [alphanumeric]
success response	code: 200 Content : {message: "Registration successful" }
error response	code: 422 UNPROCESSABLE ENTRY Content : {error: "Registration Data not correct" }
Notes	Allows a third party to register to the system.

Individual Registration

endpoint	*/auth/individual/register
method	POST
url params	
data params	username: [alphanumeric] password : [alphanumeric] name: [text] surname: [text] address: [alphanumeric] age: [integer]
success response	code: 200 Content : {message: "Registration successful" }
error response	code: 422 UNPROCESSABLE ENTRY Content : {error: "Registration Data not correct" }
Notes	Allows an individual to register to the system.

Individual Login

endpoint	*/auth/individual/login
method	POST
url params	
data params	username: [alphanumeric] password : [alphanumeric]
success response	code: 200 Content : {accessToken: [alphanumeric]}
error response	Code: 422 UNPROCESSABLE ENTRY Content : {error: "Login data not correct"} Code: 401 UNAUTHORIZED Content : {error: "Wrong username or password"}
Notes	Allows an individual to obtain an authentication Token

Third Party Login

endpoint	*/auth/thirdparty/login
method	POST
url params	
data params	VAT: [alphanumeric] password : [alphanumeric]
success response	code: 200 Content : {accessToken: [alphanumeric]}
error response	Code: 422 UNPROCESSABLE ENTRY Content : {error: "Login data not correct"} Code: 401 UNAUTHORIZED Content : {error: "Wrong VAT or password"}
Notes	Allows a third party to obtain an authentication Token

- **Third Party Controller**

Individual Request

endpoint	*/request/individual
method	POST
url params	
data params	accessToken: [alphanumeric] fiscalcode: [alphanumeric] newDataSubscription: [boolean]
success response	code: 200 Content : {message: "Requested received and ready to be forwarded."}
error response	code: 401 UNAUTHORIZED Content : {error: "Third party not logged in"} code: 404 NOT FOUND Content : {error: "Fiscalcode not present in database."} Code: 422 UNPROCESSABLE ENTRY Content : {error: "Fiscal code not correct"}
Notes	Allows the third party to do an individual request of data.

Anonymous Request

endpoint	*/request/group
method	POST
url params	
data params	accessToken: [alphanumeric] age: [alphanumeric] latCenter: [float] lonCenter: [float] radius: [float] newDataSubscription: [boolean]
success response	code: 200 Content : {message: "Requested received and ready to be analyzed."} code: 404 NOT FOUND Content : {error: "Fiscalcode not present in database."} Code: 422 UNPROCESSABLE ENTRY Content : {error: "Fiscal code not correct"}
error response	code: 401 UNAUTHORIZED Content : {error: "Third party not logged in"} Code: 422 UNPROCESSABLE ENTRY Content : {error: "Incorrect data"}
Notes	Allows the third party to do a group request of data.

Modify Third Party Password

endpoint	*/thirdParty/newPassword
method	PUT
url params	
data params	accessToken: [alphanumeric] (optional) newPassword: [alphanumeric] (optional) oldPassword: [alphanumeric]
success response	Code: 200 Content : {message: "Password changed correctly"}
error response	Code: 401 UNAUTHORIZED Content : {error: "User not logged"} Code: 403 FORBIDDEN Content : {error: "Current password provided is incorrect"}
Notes	Allows a third party to change its password.

- **Individual Controller**

Answer to Request

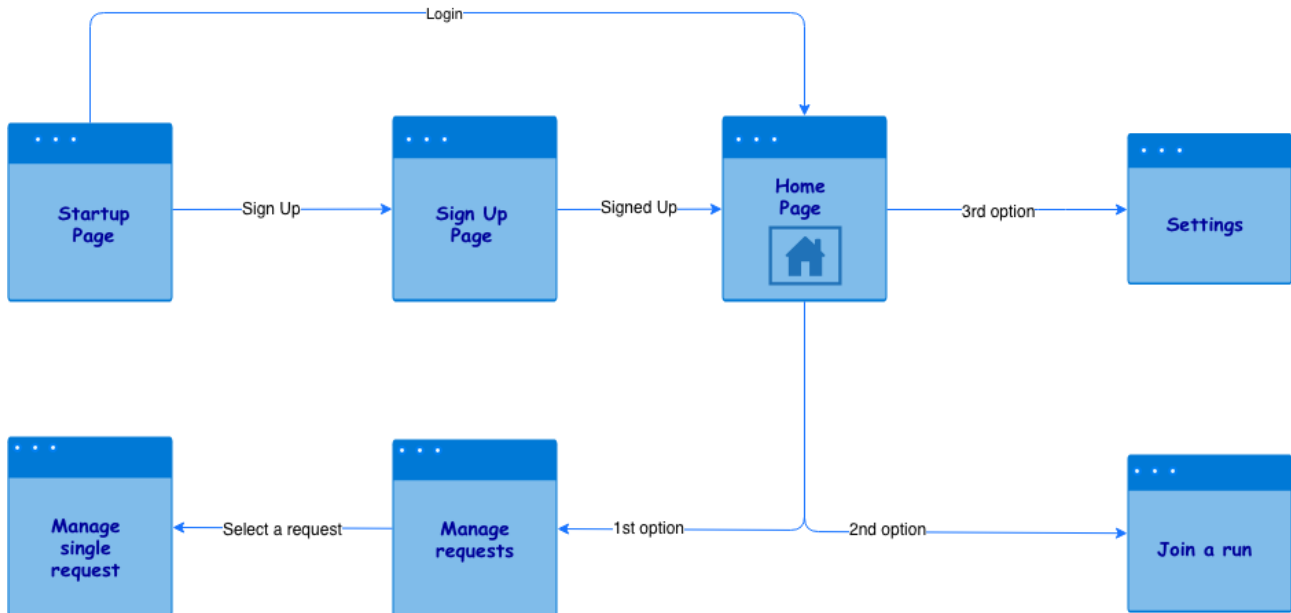
endpoint	*/answerToRequest
method	POST
url params	
data params	accessToken: [alphanumeric] thirdPartyRequester: [alphanumeric] answer: [boolean]
success response	code: 200 Content : {message: "Answer received correctly."}
error response	code: 401 UNAUTHORIZED Content : {error: "Individual not logged in"} code: 404 NOT FOUND Content : {error: "Request not found."}
Notes	Allows the individual to accept or refuse an individual request.

2.6. *Selected architectural styles and patterns*

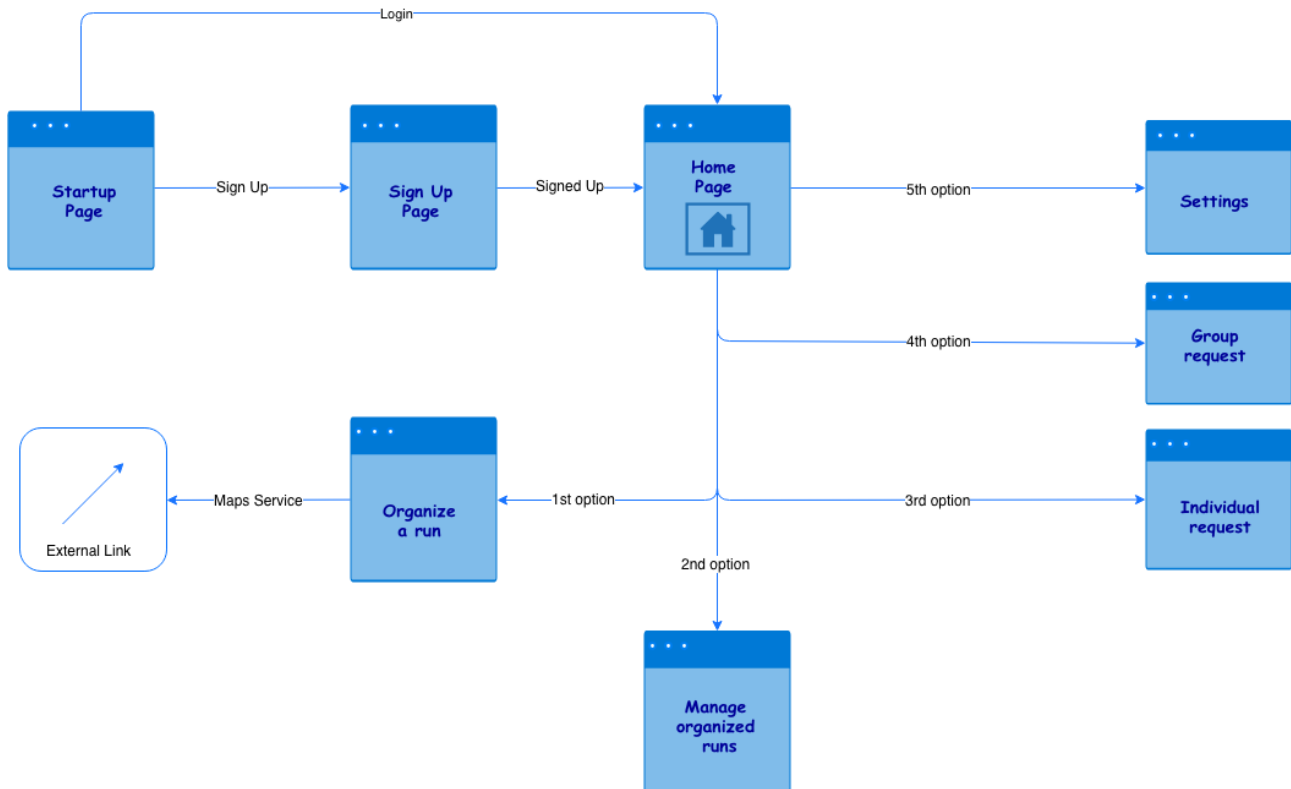
3. User interface design

3.1. UX Diagram

INDIVIDUAL UX DIAGRAM



THIRD PARTY UX DIAGRAM



For the user interface design, we refer to section 3.1.1 of the RASD document. This section is aimed to enrich what was shown in the RASD through two User Experience diagrams. Their main goal is to explain as clear as possible the relationships between the various sections of the application (addressed to

the Individuals) and the various pages of the website (addressed to the Third parties).
The two diagrams logically share the operations that allow the client to log into the application:

- Startup Page;
- Login;
- Sign Up.

Anyway, their presentation will be different due to the Mobile configuration for the Individuals and the Web based configuration for the Third Parties. The two diagrams start diverging from the principal window of the application/website, that is the Home Page. In the Individual UX Diagram, it is shown that through the Home Page the user can choose different options:

- Join a run, that allows the user to visualize the available races and select the one he wants to join;
- Manage requests, that allows the user to accept/refuse the pending requests coming from the Third parties or visualize/modify the already accepted requests;
- Open settings, that allows the user to modify his/her password, personal info, manage the connection between the smartphone and the smartwatch (or a similar device) or enable/disable the Automated-SOS service.

In the Third Party UX Diagram, the Home Page is essentially different from the other one and it allows the third party to choose the following options:

- Organize a run, that allows the third party to select the date, time and place of the event. Moreover, it is possible to select the race track thanks to the use of the Maps external service;
- Manage runs, whose goal is to allow a third party to visualize and check/modify the status of the runs organized by itself;
- Send an Individual request, through which the third party can directly ask a user for his health data, or subscribe to them;
- Send a Group request, through which the third party can ask the TrackMe system for aggregated data regarding more than 1000 users grouped by age and residence;
- Open settings, that allows the Third party to modify its password.

4. Requirements traceability

- **Third Party Controller**

- R2) The system must be able to provide to the third party the location and the health status of individuals;
- R9) The third party is not allowed to access the user's data until he/she accepts the request.
- R11) The system is optimized to send the data received from the mobile application to the third parties as soon as possible.

- **Anonymous Request Builder**

- R4) The groups must be composed at least by 1000 individuals;
- R5) The system must be able to provide to the third party the health status of individuals in an anonymous way;
- R6) The system must be able to aggregate the data of the individuals, as requested by the third party;

- **Data Retriever**

- R3) The system must be able to retrieve data from the smartwatches and similar devices;

- **Storage Controller**

- R27) The system must be able to store data retrieved from registered users.
- R8) The system must save the preference of the user;

- **Individual Controller**

- R1) The users must have given the consensus to the treatment of their information to the third party;
- R28) The user must have an active subscription to stop it;
- R29) The system must be able to allow the user to unsubscribe to the third party and to stop the transmission of his/her data.
- R7) The system must be able to forward the requests from the third party to the user;
- R26) The system must allow the user to enable/disable the AutomatedSOS service at any time.
- R31) The system must allow the user to change his/her personal info.

- **Authentication Controller**

- R12) The users must provide their personal data to the application during the registration process, SSN (or fiscal code) included;
- R13) The system must allow the user to register to the application by selecting a username and a password;
- R14) The system must allow the user to log in to the application by providing the combination of a username and a password that matches an account;

- R15) Two different users cannot have the same username.
- R16) The system must allow the third party to register to the application, by specifying its VAT registration number and a password;
- R17) The system must allow the third party to log in to the application by providing the combination of a VAT registration number and a password that match an account;
- R32) The system must allow the user to change his/her password.
- R33) The system must allow the Third party to change its password.

- **Track4Run User Controller**

- R19) The system must be able to retrieve the position of all the runners;
- R20) The system must be able to provide the position of all the runners in the track in real time.
- R21) The system must allow the user to check the list of available races at any time.
- R22) The system must allow the user to join an available race only before its starting time.
- R23) The user cannot join two different overlapping races.
- R30) The system must avoid the registration of users after having reached of the maximum number of participants.

- **Track4Run Third Party controller**

- R19) The system must be able to retrieve the position of all the runners;
- R24) The system must allow the third party to organize a race by defining its track and its time.

- **Health Checker**

- R18) When the health status values go below the threshold, the system must send an SOS within 5 seconds.
- R25) The AutomatedSOS service must be enabled.

- **Mobile Controller**

- R34) The system must allow the user to connect a smartwatch or a similar device to its smart-phone.

5. Implementation, integration and test plan

In section 2.2 of this document there is the description of the components in which the whole system can be divided to split roles and functionalities and to simplify the development and the following testing. As it is evident from the Component Diagram, the components can be classified into the following subsystems:

- Mobile client, made up by:
 - Components: Mobile controller, Data retriever, Health checker, Presentation mobile;
 - Interfaces for external services: Map service interface, OS Bluetooth interface, Smartwatch interface, OS call service interface.
- Web client;
- Business logic, made up by:
 - Components: Individual controller, Third party controller, Authentication controller, Track4Run Individual controller, Track4Run Third party controller, Anonymous request builder, Storage controller;
 - Interfaces for external services: Map service interface.
- External components: Map service, OS Bluetooth service, OS call service, Smartwatch service, DBMS.

A bottom-up strategy will be used to implement, integrate and test the system. Then the following steps will be performed:

1. each subsystem will be implemented, integrated and tested;
2. the subsystems will be integrated and tested together.

Since we cannot directly manage external components, we assume they are reliable and we use the provided interfaces to test our system.

To keep the integration and testing process more clear we can split the Business logic subsystem into the following subsystems:

- Individual subsystem: Individual controller and Storage controller;
- Authentication subsystem: Authentication controller and Storage controller;
- Thin third party subsystem: Third party controller and Storage controller;
- Full third party subsystem: Third party controller, Anonymous request builder and Storage controller;
- Track4Run individual subsystem: Track4Run individual controller and Storage controller;
- Track4Run third party subsystem: Track4Run third party controller and Storage controller.

To reach the same goal, in the Mobile client subsystem we can distinguish:

- Data4Help subsystem: Data retriever and Health checker;
- Transfer data subsystem: Data retriever and Mobile controller.

Focusing the attention on the Mobile client, after having implemented and tested all the subsystems (step 1), it is needed to test the integration of all of them. Let's call the result Mobile client subsystem.

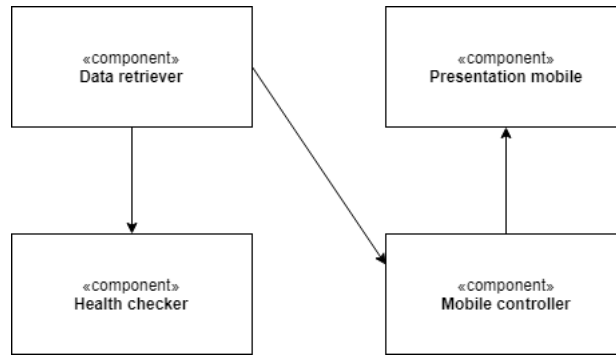


Figure 1: Mobile client subsystem

Coming to the server side, after having implemented and tested all the subsystems, it is needed to test the integration of each of them with the Mobile client subsystem and with the Web client component. More in detail:

- Mobile client subsystem and Individual subsystem;
- Mobile client subsystem and Authentication subsystem;
- Mobile client subsystem and Track4Run individual subsystem;
- Web client component and Authentication subsystem;
- Web client component and Full third party subsystem;
- Web client component and Track4Run third party subsystem.

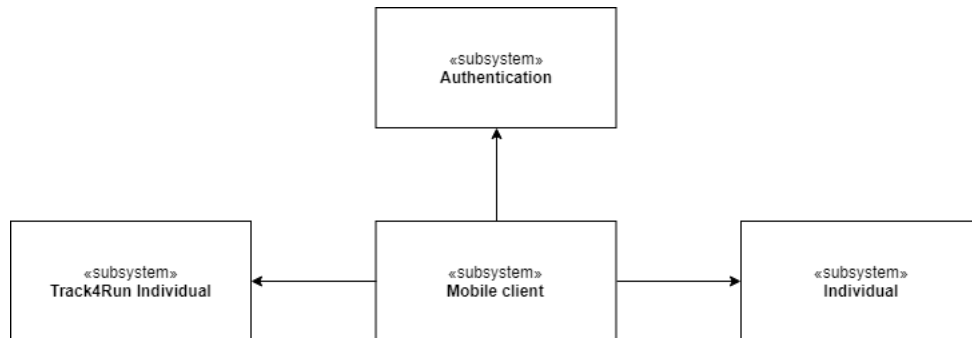


Figure 2: Mobile client tested with the other subsystems

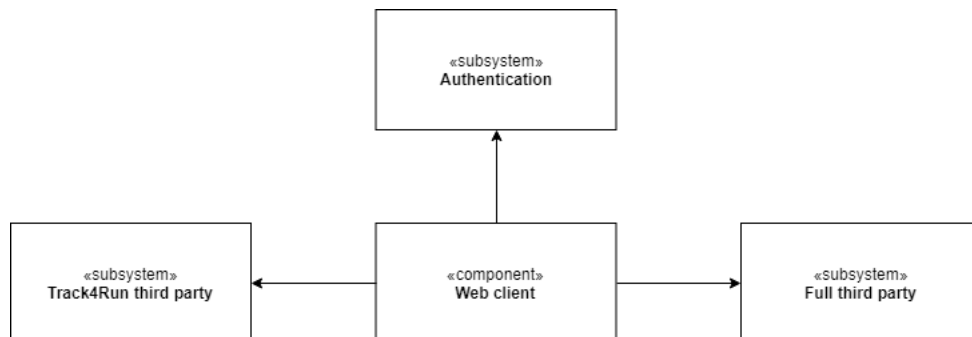


Figure 3: Web client tested with the other subsystems

After all the previous tests, a full integration test can be performed.

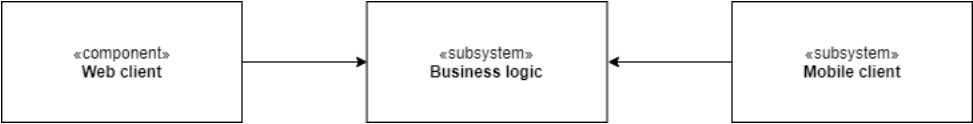


Figure 4: Test of the whole system

6. Effort spent

- **Paolo Romeo**

Description of the task	Hours spent
Architectural design	7
User interface design	2
Requirements traceability	2
Implementation, intergration and test plan	6
Correction of the RASD	3
Other related activities	5

- **Andrea Scotti**

Description of the task	Hours spent
Architectural design	8
User interface design	2
Requirements traceability	2
Implementation, intergration and test plan	6
Correction of the RASD	2
Other related activities	5

- **Francesco Staccone**

Description of the task	Hours spent
Architectural design	7
User interface design	4
Requirements traceability	2
Implementation, intergration and test plan	5
Correction of the RASD	3
Other related activities	4

7. References