Politecnico di Milano

AA 2018/2019



DD – Design Document

Version 1.0 - 11/12/18

*Authors: Professor:*

Emilio Imperiali Elisabetta Di Nitto

Giorgio Labate

Mattia Mancassola

1. **Introduction**

1.1 Purpose

The purpose of this document consists of giving more technical details than the RASD concerning the TrackMe application.

Indeed, if the RASD has as its objective to provide a more abstract view of the system with its functionalities, the Design Document goes deeper into detail about the implementation, providing an overall guidance to the architecture of the project. Here all the components forming part of the system are described, with the related run-time processes, the algorithms which are the basis of the application are explained and all the implementation choices are listed and motivated.

In particular, the following topics are touched by the document:

* The high level architecture;
* The main components and their interfaces;
* The runtime behavior;
* The design patterns;
* The algorithms’ design for the most crucial ones;
* Implementation plan;
* Integration plan;
* Testing plan.

1.2 Scope

<here goes more or less the same general purpose/scope which is in the RASD>

1.3 Definitions, acronyms, Abbreviations

1.3.1 Definitions

<TODO>

1.3.2 Acronyms

* API: Application Programming Interface
* DD: Design Document
* RASD: Requirements Analysis and Specifications Document

1.3.3 Abbreviations

<TODO>

1.4 Revision history

* Version 1.0:
  + First Release

1.5 Reference documents

<TODO>

1.6 Document Structure

**Chapter 1** is an introduction to the design document. Its goal is to explain the purpose of the document and to highlight the differences with the RASD, whilst showing the link between them.

**Chapter 2** aims to provide a description of the architecture design of the system. More precisely, this section is divided in the following parts:

* Overview
* Component view
* Deploying view
* Runtime view
* Component interfaces
* Chosen architectural styles and patterns
* Other design decisions

**Chapter 3** describes the design of the algorithms which represent the core of the application’s functions. In order to remain above the implementation’s details, they are outlined with pseudocode, also to facilitate greater understanding.

**Chapter 4** specifies the user interface design. Actually, this part is already contained in the RASD in the mockups’ section, so here will be added only additional behaviors.

**Chapter 5** provides the requirements traceability, namely how the requirements identified in the RASD are linked to the design elements defined in this document.

**Chapter 6** includes the description of the implementation plan, the integration plan and the testing plan, specifying how all these phases are thought to be executed.

**Chapter 7** shows the effort which each member of the group spent working on the project.

1. **Architectural Design**

2.1 Overview: High-level components and their interaction

The application to be developed is a distributed application and the three logic software layers of Presentation (P) that manages the user interaction with the system, Application (A) that handles the business logic of the application and its functionalities and Data access (D) that manages the information are thought to be divided on three different hardware layers (tiers) that represent a machine (or a group of machines) so that any logic layer has, in principle, its own dedicated hardware: we have a so called three-tier architecture. This architecture is thought to guarantee to the system characteristics of scalability and flexibility and to lighten the server side splitting it into two nodes. In particular, the second tier is thought to contain only the business logic to physically separate users and data to guarantee more safety in accessing to data since the system deals with sensitive data.

The following image show the high-level architecture of the system without providing any detail.



Figure 1 – High-level system architecture

For what concerns the third parties, they can communicate through their devices with the application level to make queries and to organize competitions with a synchronous message flow (the server implementing the business logic have to provide an answer). The server of the application level will interact with the customers also when sending notifications (SOS etc.) in an asynchronous way (they don’t wait for an answer). Instead, for what concerns the users, they interact with the application level providing answers to queries and their data (asynchronous messages) and to retrieve their data and stats, enroll themselves for competitions or watch them (synchronous messages). Finally, the server in the application layer communicates synchronously with the database server (data access layer) to retrieve or store information when needed. (TODO -> storing data is asynchronous?)

To augment the system scalability a scale-out approach is followed: performances improvement is obtained through nodes replication. This approach, that requires the adding of a load-balancing system to distribute the working load among the various nodes, allows to exploit the downsizing principle that affirms that low-end servers have minor costs of high-end servers for the same computational power. Moreover, cloning with shared disk configuration: clones share the memory disks (shared nothing configuration is not convenient since the offered service is very ‘write intensive’) is exploited both to distribute computational load and to replicate data for security reasons. So, this technique increase both scalability properties and faults tolerance of the service and is important in particular for the critical service offered through AutomatedSOS. Finally, to guarantee an appropriate packets control, firewalls are installed before and after the application tier to create a DeMilitarized Zone (DMZ) for the application servers so that the external network can access only to the resources exposed in the DMZ. The web servers don’t guarantee the same security level and this is another reason why, in general, they forward the requests to the application servers in the DMZ.

A more detailed, but still informal view of the system is provided in the following image.

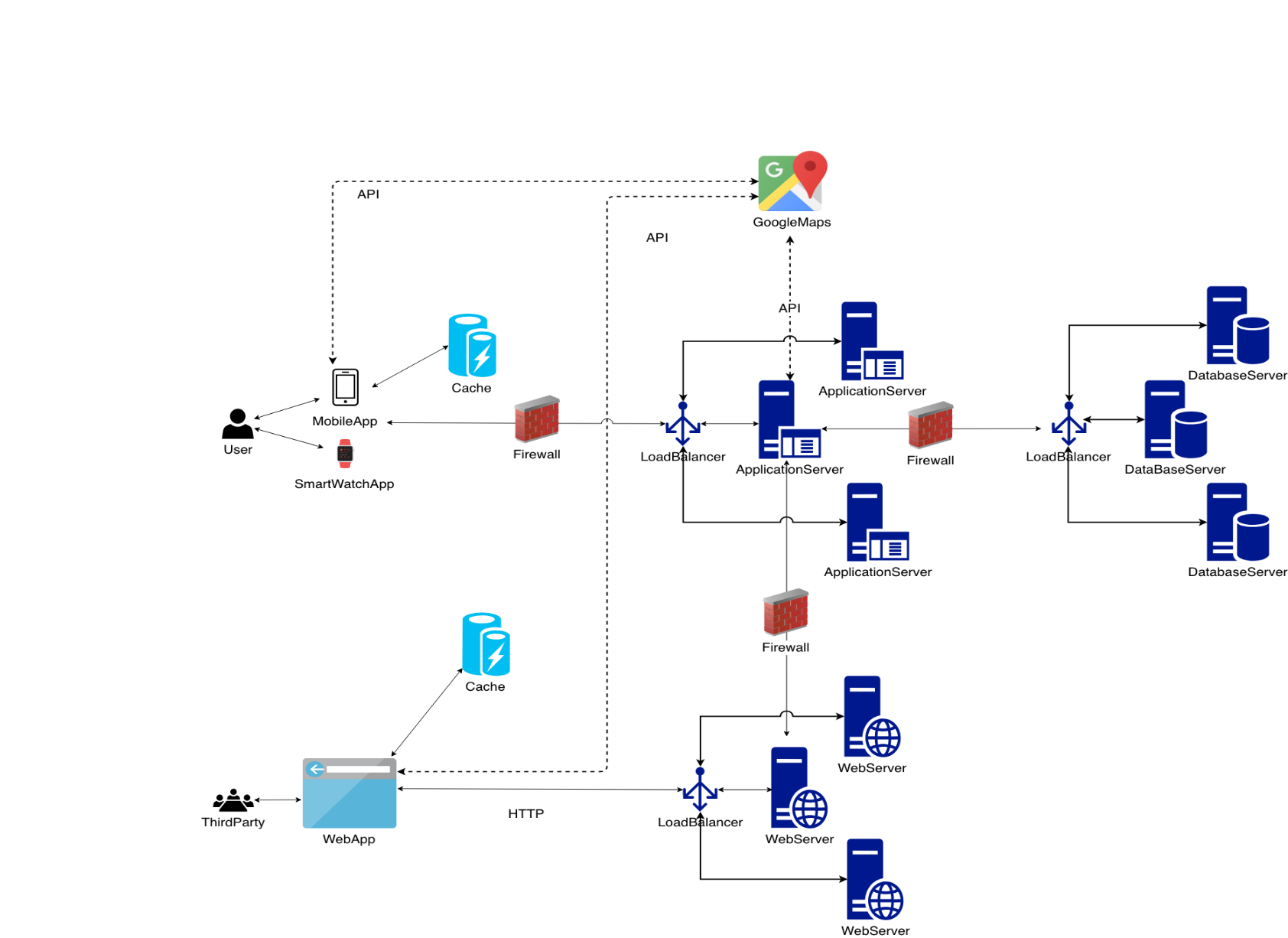


Figure 2 – System Architecture

In the Application tier we have an application server to provide the customers with access to the business logic which generates dynamic content (customable, extensible, interactive and seamless). Then we have a Web server to work with the HTTP standard in case of communication with the third parties’ web application, but to lighten its load the Web server is not supposed to generate dynamic content through plugins for scripting languages: it will forward the requests to the Application server if that is the case. To fasten and lighten the communication, caches are used in front of the Application tier: the cache needs to have an appropriate knowledge of data that make up the business objects data, business logic and changes that can transform them at UI level: this knowledge is required to invalidate data when needed (some alterations occurred). [Moreover the users’ mobile app stores part of the users’ data and stats (most recent ones and manually inserted ones) in their dispositive so that they do not even have to be connected to the Internet to consult their data and stats.] TODO 🡪 non è proprio questo che fanno le caches?

It is worth to note that caches for applications servers can’t be exploited because of node replications: it is not possible to know what have been requested from a certain application server and what from another one so it is impossible to provide a cache that would prevent them from accessing the database server every time.

Finally TrackMe exploits data mining techniques to exploit the big quantity of data available and extract from them relevant information and recurrent patterns that can be useful for the third parties that want, for example, find ‘hidden’ information and characteristics about their own clients or, more generally, about certain sets of TrackMe’s users. This can be obtained through various learning techniques: association rules, classification and clustering.

2.2 Component View

The following diagram contains all the components (logical or physical ones) of the system showing their interactions. The ports that represent the external interface exposed by components are shown only among different subsystem for the sake of simplicity.

In the diagram only the application server subsystem is analyzed in detail because it is the core component of the system: it contains the business logic. The other components of the presentation layer, of the data access layer and the web server are represented (through their software components only) just to represent their interactions with the application server.

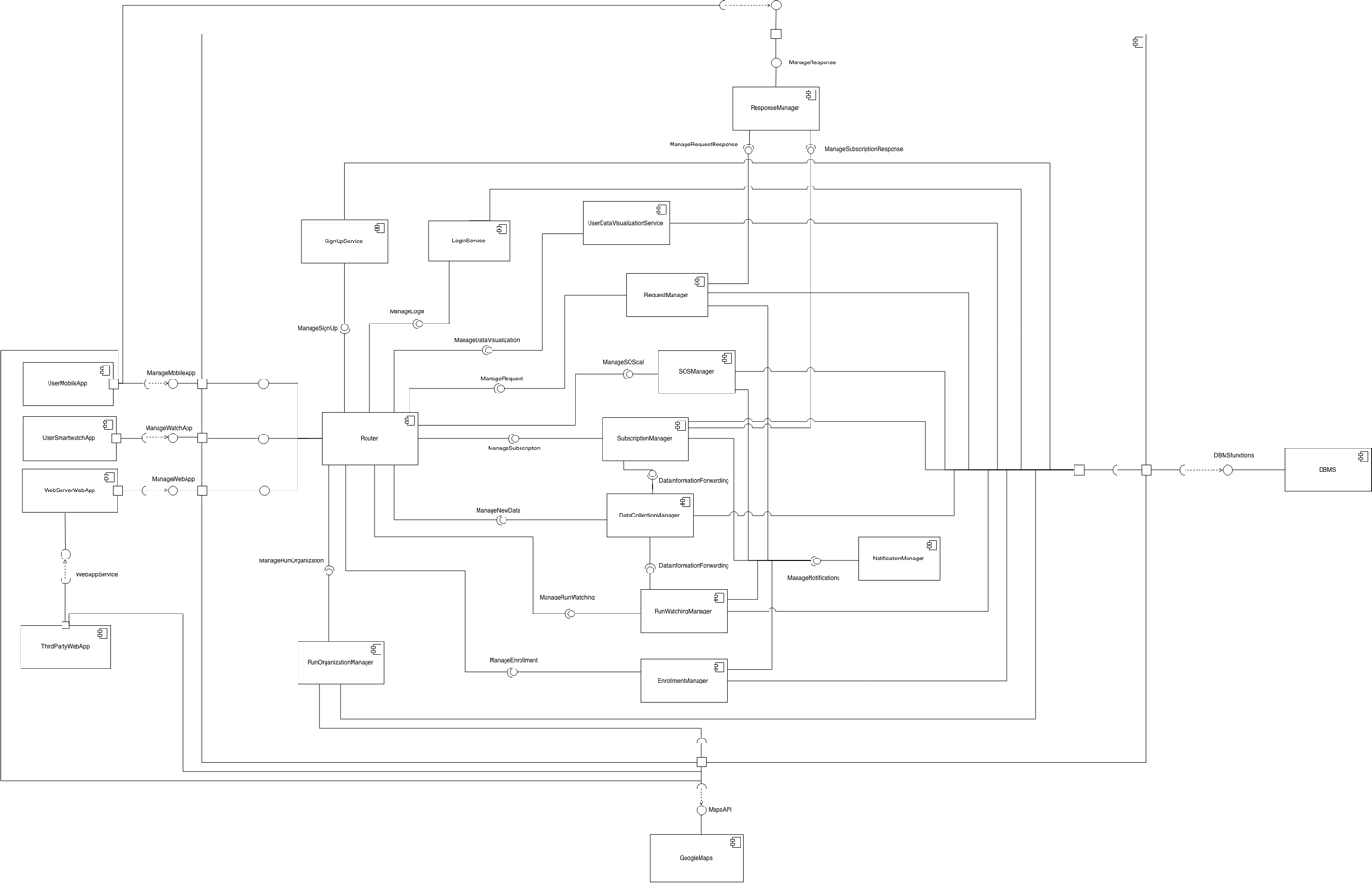


Figure 3 – Component Diagram

The components’ functions contained in the application server are described in the following:

* **Router**: it manages all the ‘messages’ and all the function call coming from the other subsystems to pass the data to the correct component and eventually call the right method/function on it. The router is partitioned according to the type of component it has to interact with because the functionalities offered are quite different among them. The **MobileAppRouter** handles the interaction with the users’ smartphone app: it allows them to sign up, to login, to consult their own data and stats and to watch or enroll for a run. This component also forward the received data (all the data among the required ones that a smartphone is able to collect) to the ‘DataCollectionManager’ in the case that the smartwatch is turned off. The **SmartwatchAppRouter** is indeed concerned with messages coming from the users’ smartwatches (by default data are collected only through them unless the device is turned off): it has to forward the received data to the ‘DataCollectionManager’ and to forward the SOS call in case of emergency to the ‘SOSManager’. Finally the **WebAppRouter** offers the interface for the interaction with third parties’ web application: it must forward to the appropriate components the login and sign up data, the individual and aggregate requests, the subscription requests and the data concerning the organization of a run. A more detailed view of the Router component to show this is provided below.

Figure 4 – Detailed view of the Router component



Figure 5 – Detailed view of the Router component’s interfaces

* **SignUpService**: this component contains all the procedures to allow the customers to register to TrackMe expressing also to which service they want to register for. It has to interact with DBMS to store data about the registration and performing controls about the chosen username and password.
* **LogInService**: it manages all the logic inherent to the authentication of the customers. It interacts with the DBMS to check that the authentication parameters match the stored ones.
* **UserDataVisualizationManager**: it comes into play when the user wants to access to its own data and stats, for example accessing at his own monthly stats about heartbeat. It contains the applicative logic to handle the requests and provide the correct answers and has to invoke the DBMS to retrieve from the database the requested information.
* **RequestManager:** this component deals with requests by third parties about single individuals or groups of individuals. It has to retrieve the requested data from the database (has to interact with the DBMS), make the privacy controls in case of aggregate requests, forward the queries to the requested users, handle their answers in case of individual requests and provide the right feedback to the requesting third parties.
* **SubscriptionManager:** it contains all the logic about subscriptions to users’ data for the third parties. It handles the requests for subscriptions for individual users or groups, the provided answers for the subscription and it is concerned in forwarding the data as soon as they are produced in case of a successful individual or group subscription (it provides an interface to the ‘DataCollectionManager’ to be able to do this).
* **SOSManager:** this component receives the emergency call from the user’s mobile app and is concerned in finding the third party that is nearer to the user to forward to it the SOS. The control to check if parameters are out of the defined bound is performed client side, this component is concerned only in handling the emergency call (this is why it offers its interface only to the ‘Router’ and not to the ‘DataCollectionManager’).
* **RunWatchingManager:** this component is concerned in providing to all the willing users the possibility to follow a desired run. It receives continuously information from the ‘DataCollectionManager’ about the new collected data and, analyzing them, it is able to perceive which of them must be retrieved from the database and to which users they have to be forwarded. It exploits the ‘NotificationManager’ to remind with one hour in advance that the competition for which the user has expressed the will to watch is beginning in short time.
* **EnrollmentManager:** it manages all the requests of enrollment to organized competitions. This component has only to verify the availability for the requested run and send the confirmation to the requesting user providing him with an identifier for the competition he has enrolled for. It exploits the ‘NotificationManager’ to remind with one day in advance about the competitions for which the user has enrolled.
* **RunOrganizationManager:** it deals with the organizations of a competition asked by some third party. This component has to verify that all the inserted data are correct, for example it has to control that the defined path is feasible, that it doesn’t cross an already defined path for another defined competition in the same time slot and this kind of things (that’s why it has to exploit Google Maps APIs).
* **DataCollectionManager:** this component receives all the data transmitted by users and has to forward the proper information about them (meta-information to the other components needing them that are the ‘SubscriptionManager’ and the ‘RunWatchingManager’ so that they can retrieve the eventually needed data from the database).
* **NotificationManager:** this component deals only with the logic for push notifications, it sends to the customers only asynchronous messages (doesn’t expect for any feedback by them). All the other components that have to forward some message to a client (for example the ‘RequestManager’) has to exploit the interface offered by this component. This component has been conceived to maintain single responsibility of the components: the type of messages sent are asynchronous (they are different from the general response messages provided by the server) and so it is more correct to use a different component rather than sending push notifications directly from the components where they were originated. When a notification is sent the dedicated client’s interface in ‘ResponseManager’ for the handling of the client’s response is provided (in our system this happens in case of a request of subscription or individual request). This mechanism of providing the interface of ‘ResponseManager’ only when ‘needed’ is exploited to show the interface only to authorized clients (i.e. clients that have to response to a request sent as an asynchronous notification).
* **ResponseManager:** this component is the handler of the client’s answer to a request of subscription or to an individual request and, in general, for all the responses that a client will eventually be able to provide if some new functionality will be introduced in future versions of the system.

It is important to notice that the only components that exploit the APIs offered by Google Maps are the clients’ ‘UserMobileApp’, ‘ThirdPartyWebApp’ and the ‘RunOrganizationManager’ on the server side: this is because all the visualization and interaction tools offered by Google Maps’ APIs have to be directly encoded on the clients’ app and on the application server the APIs are exploited only for the functionalities concerning the organization of a competition (ex: checking if two paths overlap in some point in the case of simultaneous competitions).

2.3 Deployment View

In the following image the TrackMe deployment diagram is represented: it shows the execution architecture of the system and represents the distribution (deployment) of software artifacts to deployment targets (nodes). Artifacts, in general, represent pieces of information that are used or are produced by a software development process and are deployed on nodes that can represent either hardware devices or software execution environments.

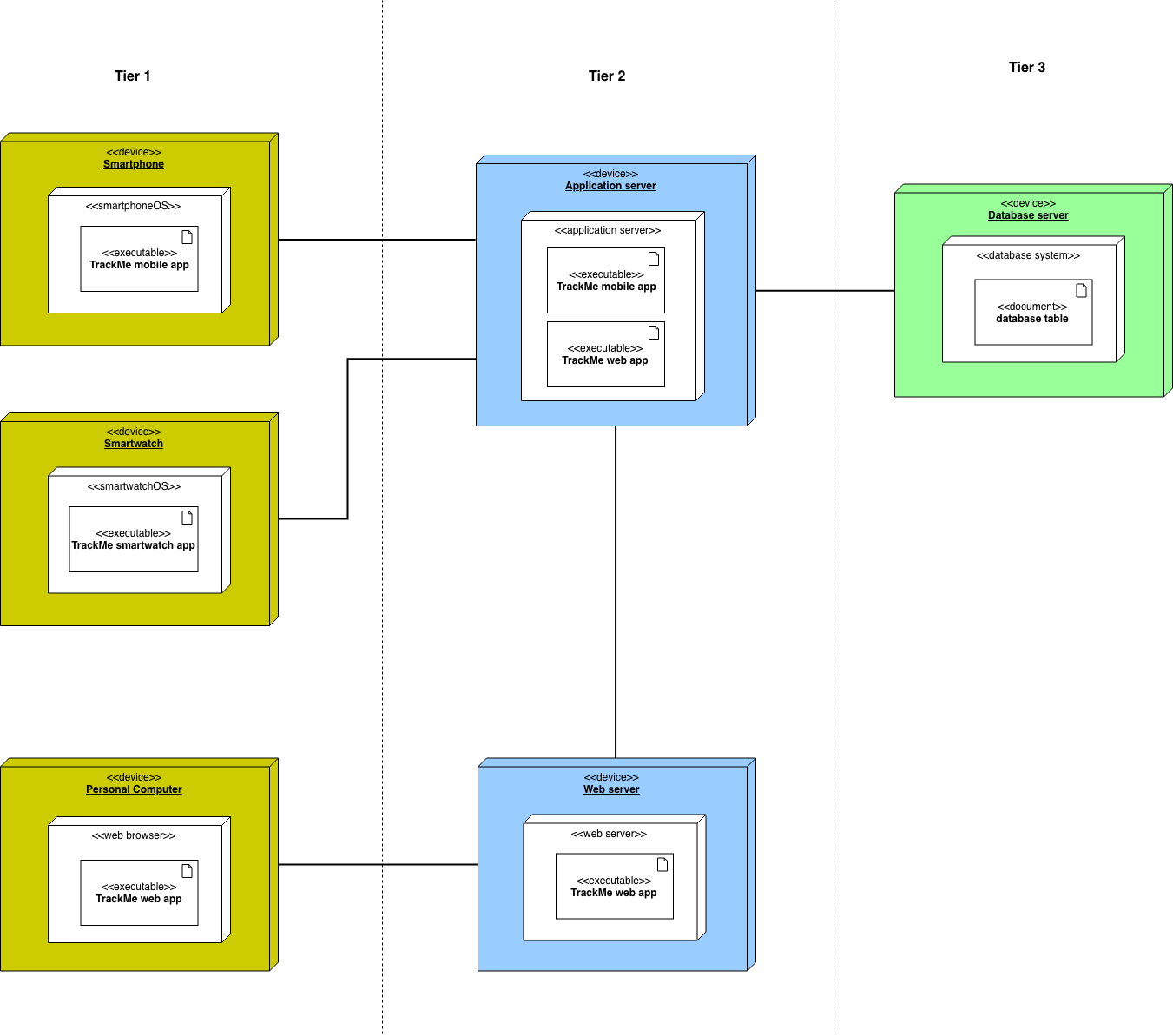


Figure 5 – Deployment Diagram

[TODO: explain why we decided to use mobile app and web app]

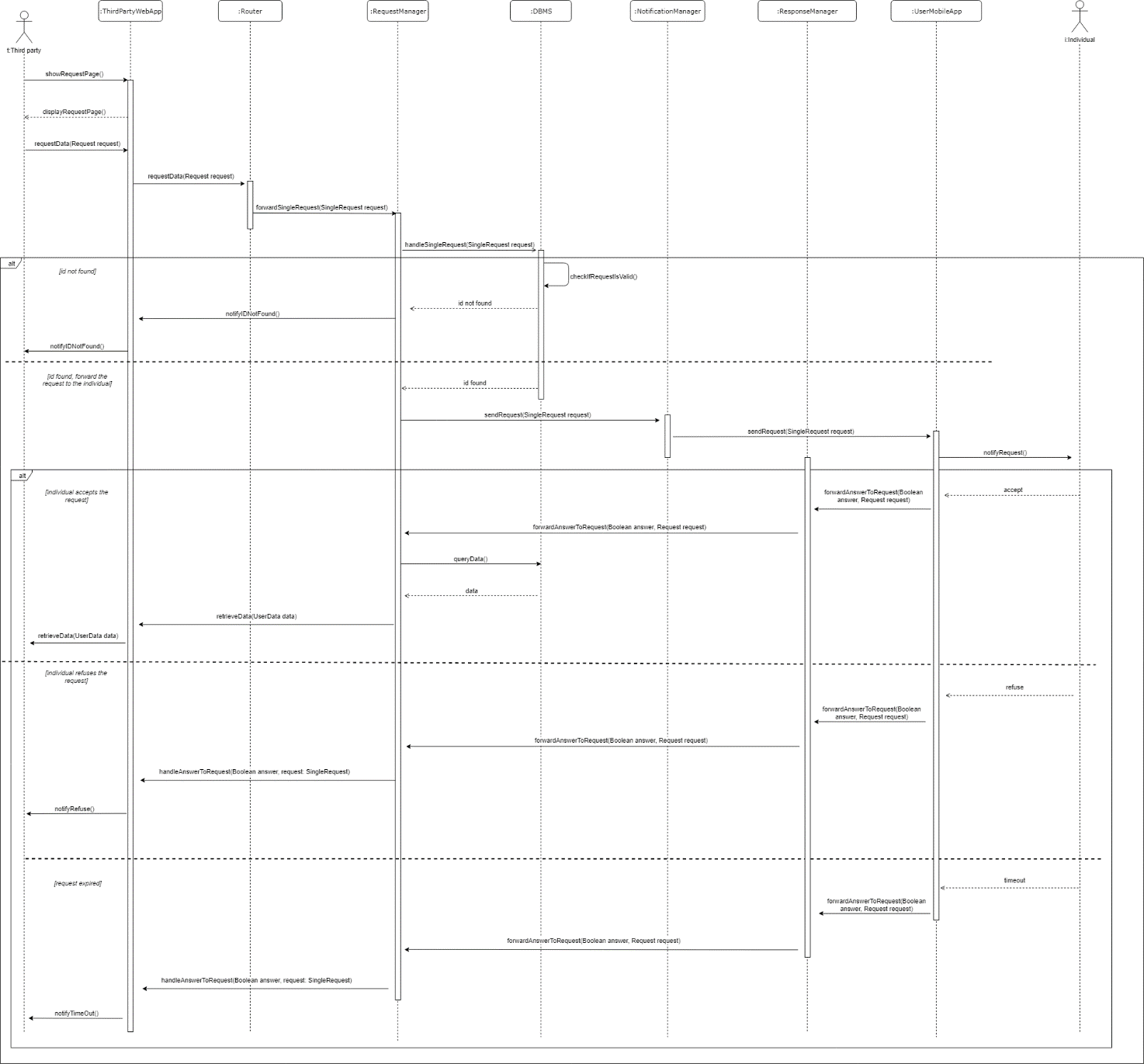
In the diagram ‘<<executable>>’ and ‘<<document>>’ are standard UML stereotypes that apply to artifacts: the former represents a program file that can be executed on a computer system while the latter represents a generic file that is not a «source» (another UML standard stereotype) file or «executable», in this case it represents the tables in the database.

In the diagram external systems as well as some other components (like load balancers and firewalls) are not represented to focus only on the components that host the core functionalities of the application or to components for which the deployment is effectively executed (Google Maps is already built and deployed). The three tier respectively contains:

* Tier 1: here the presentation logic must be deployed. Users must be provided with a mobile application on their smartphone and third parties with a web application accessible from their web browsers. Users communicate with the application server to retrieve their own data and stats, to report an emergency or to enroll or follow a competition. Third parties communicate with the web server to retrieve users’ data, receive emergency reports or organize run competitions.
* Tier 2: here is deployed the application logic. The application server implements all the business logic, handles all the requests and provide the appropriate answers for all the offered services. It is directly addressed by the mobile application and handles also some requests that are forwarded by the web server and sent by the web application in all the cases in which the web server can’t provide information either because it doesn’t have them in its local disk or because some dynamic content has been requested.
* Tier 3: here the data access must be deployed. The database server is conceived to execute a relational DBMS (RDBMS), the database is relational. This is because the structure of a relational database allows to link information from different tables through the use of foreign keys (or indexes), which are used to uniquely identify any atomic piece of data within that table and this is very important for applications that are heavy into data analysis like TrackMe. Moreover the application has to handle a lot of complicated querying, database transactions and routine analysis of data and for all these reasons a relation approach is what is needed. A non-relational database would be inappropriate because it would not be able to represent some structures (as the users’ account etc.): it can’t express rules and constraints and have no fixed structure.

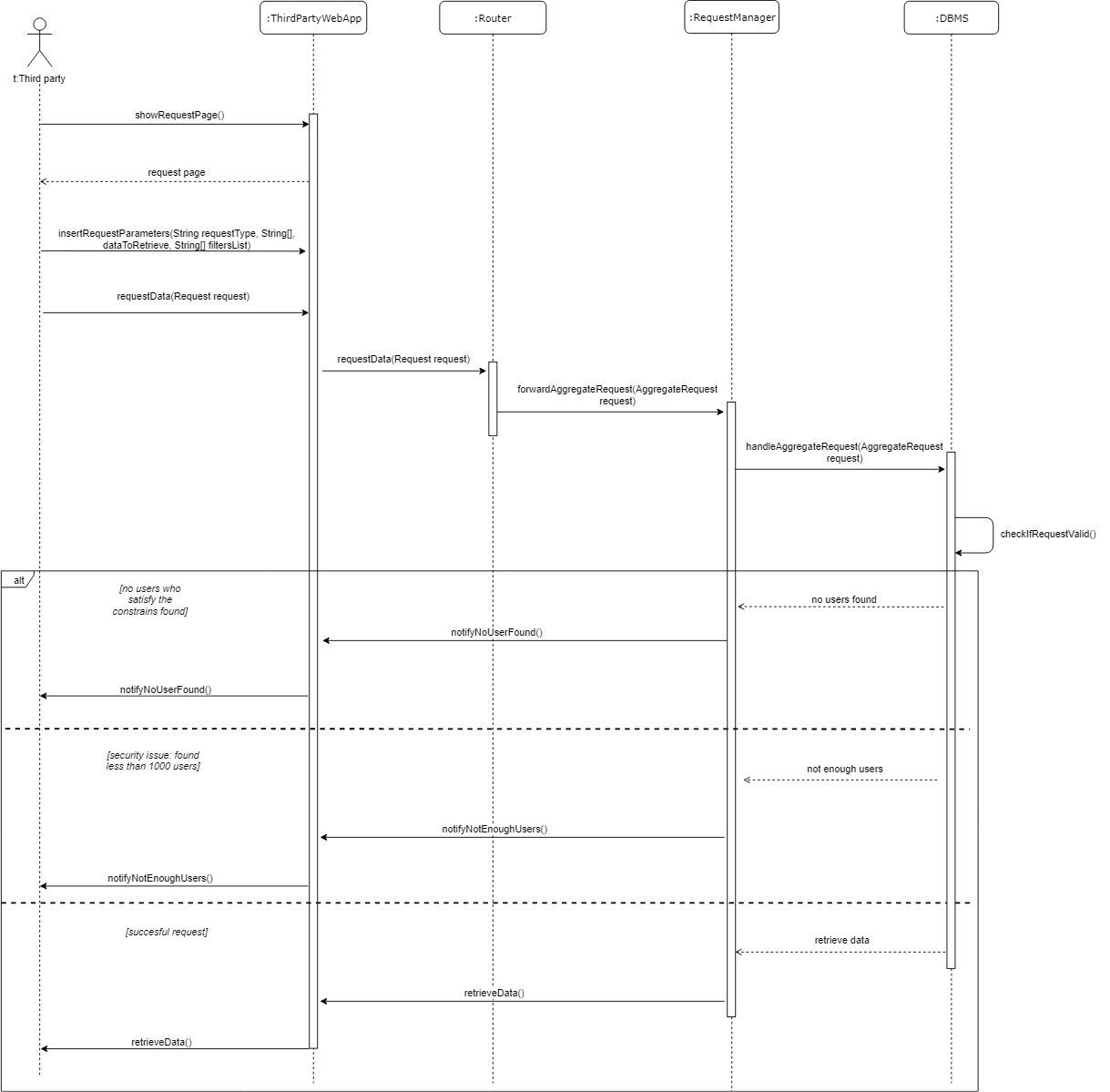
2.4 Runtime View

2.4.1 Individual request



In this sequence diagram it is shown the process through which a third party can request the data of an individual. Once the web app has rendered the page for making the request, the third party can insert all the needed input data to perform the action (the data are here thought to be contained in the Request object). When submitted, the request is sent to the Router, which forwards it to the right component, i.e. the Request Manager. The latter is responsible for checking, communicating with the DBMS, if the request is valid: if the requested id does not exist in the database, an error message is sent back to the third party. Otherwise, if the check goes through, the Notification Manager is in charge of warning the individual. At this point, the user can decide whether to accept the request or not. There is a specific component in charge of receiving the user’s response, the Response Manager, which talks to the Request Manager. The Request Manager, then, according to the user’s decision, either queries the database for retrieving data or forwards to the third party a message which contains the user’s refusal. There is also a third case, which plays its part when the user doesn’t answer to the request within a time limit of 24 hours.

2.4.2 Aggregate request



In this sequence diagram it is shown the process through which a third party can request the data of a group of users, on the basis of some criteria. At first the flow is similar to the individual request one, the third party asks for the request page and when this is rendered, it can insert the parameters. Of course here the difference is that there are no identifiers, but only a bunch of filters, which the third party can choose to select a specific population. Once the needed data are inserted, the request is sent to the Router and then forwarded to the Request Manager, which talks to the DBMS to check its validity. Here three scenarios can occur:

* There is no user who satisfies the selected criteria in the database; in this case the third party is notified with a dedicated message.
* There aren’t enough users who satisfy the selected criteria in order to guarantee their privacy, i.e. the query’s result contains less than 1000 rows.
* The query goes fine and the data are retrieved to the third party.

2.6 Selected architectural styles and patterns

1. **RESTful architecture**

To develop the application we decided to use a RESTful architecture, with the goal to reduce the coupling among client and server components as much as possible in mind and also because the centralization of data plays an important role. Moreover, it fits very well for the scope since we are dealing with an application with many clients, on which we don’t have control, while on the contrary we have it on the server and we may want to be able to update it regularly, without touching the client software.

Using a RESTful architecture inevitably leads to an adoption of the following constraints:

* Uniform interface
* Client-server
* Stateless
* Cacheable
* Layered system

Concerning the client-server architecture, the third party will use the appropriate web app, which communicates with the web server, which in turn communicates with the application server. The user, instead, will use the mobile application to access directly the application server.

Finally, the application server acts like a client, querying the database server.

1. **Three Tier Client-Server**

We choose a multitier architecture because it allows to decouple the complexity of the system, making it more flexible and reusable. Indeed, the developers acquire the power of modifying or adding specific layers without disrupting the entire application.

More precisely, we adopted a three tier architecture, composed of a presentation tier, a domain logic tier and a data storage tier.

1. **Model View Controller (MVC)**

We decided to use this pattern in order to guarantee the reusability of code and also to promote a parallel development as much as possible.

MVC, indeed, with the separation of concerns allows flexibility and opens up the doors to other design approaches, which without it would be difficult to use.

In our case, the clients represent the front-end, i.e. the view, that interact with the controller, through which the information flows to and from the database, namely, the model.

**Other design decisions**

Thin client

We opted for a thin client to maintain the line of thought underlined till now. Indeed, this allow us to have an architecture in which the client is designed to communicate with a server, where the real logic is implemented.

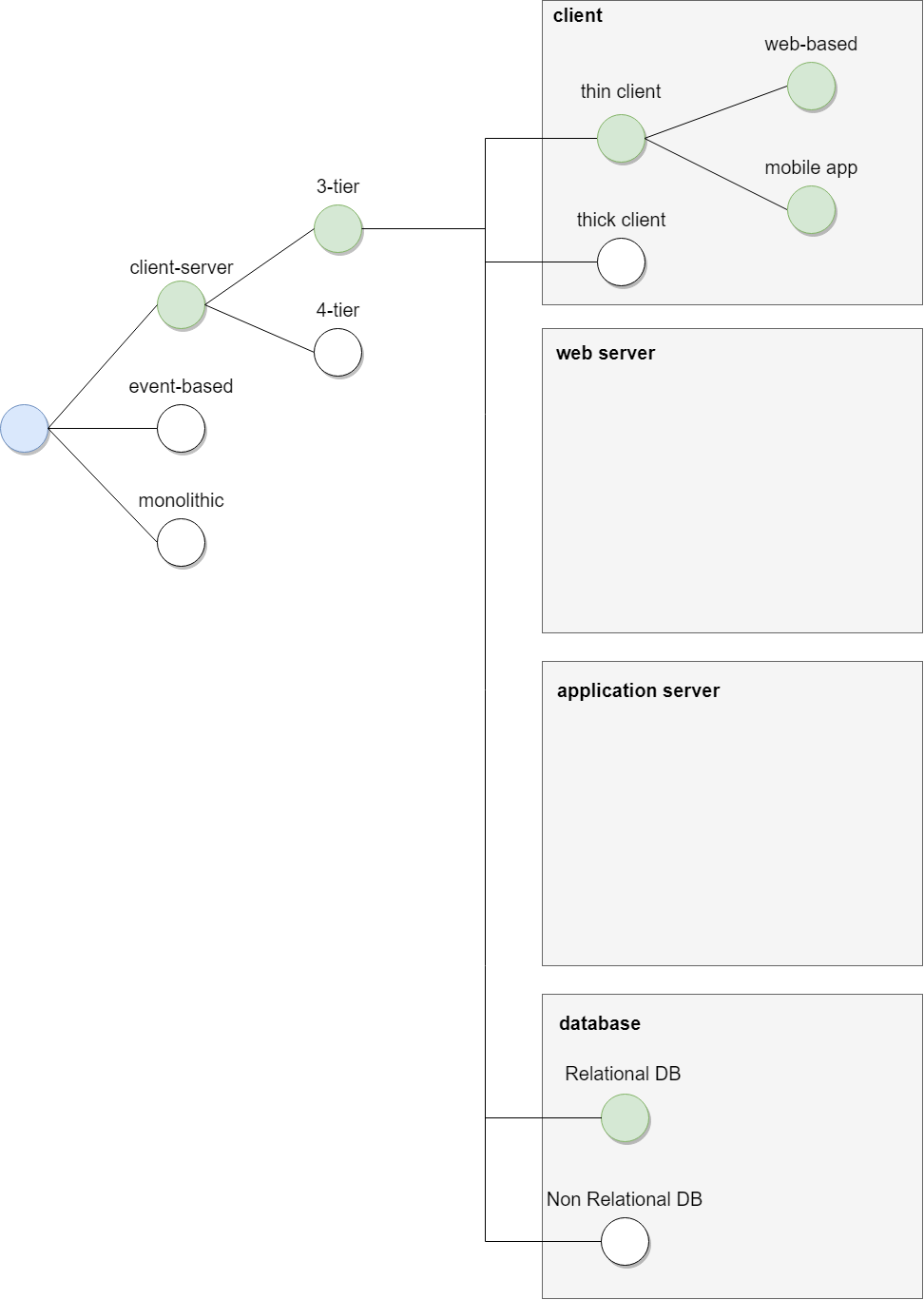
Thin clients are strictly dependent on a network connection, however in our case the application was conceived to be online, so this is not an issue. Of course on the other hand this means that the connection must be fast and reliable in order to guarantee a high quality service to the users.

It is worth mentioning that there is one exception, which consists of using the Google Maps API internally to the client when the service which allows to watch a run and visualize the runners in real time on the map is in use. This has been decided to avoid to overload the server.

Relational database

Relational databases are a good choice when there is the need to deal with several transactions and when the data are linked by some relationships (users, third parties, runs etc.). This fits perfectly for our purposes, which can be catalogued as data analysis.

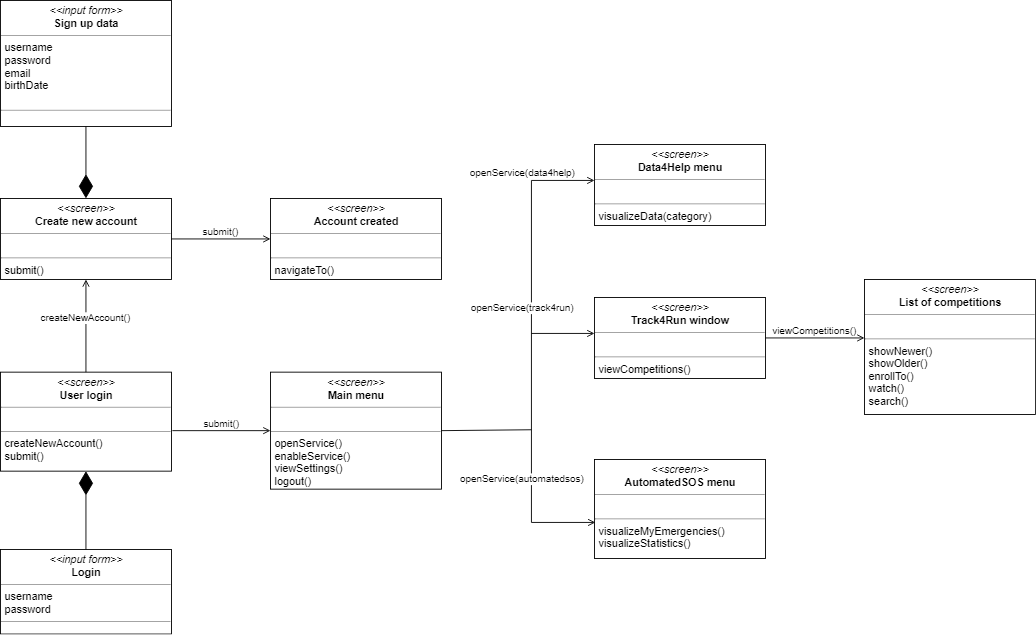
<Other more low level design patterns, like façade or observer>



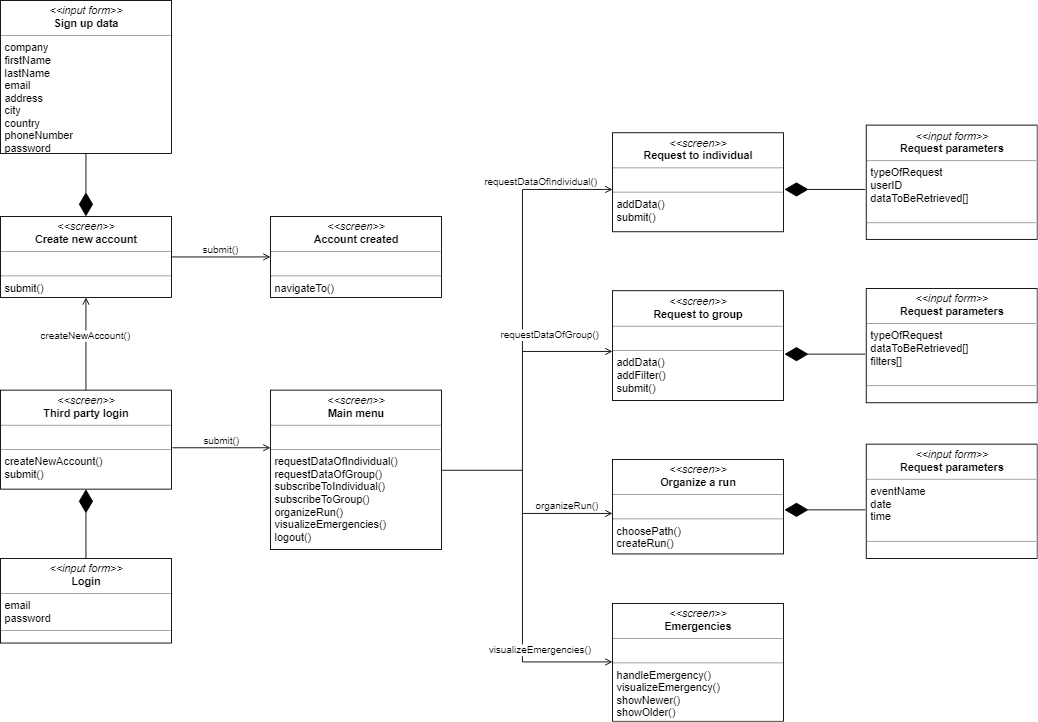
Decision Tree

1. **User interface design**

The mockups of the application were already exposed in the RASD document in the appropriate section. Here we present two UX-diagrams to show how the customer is supposed to navigate inside the application. We chose to expand only some of the possible interactions, to avoid to overcomplicate the diagram.



UX diagram- User

****

UX diagram- Third Party

1. **Requirements Traceability**

The whole design has been thought to guarantee that the system is able to enforce the requirements defined in the RASD (and, as a consequence, to achieve the prefixed goals). Here a mapping between those requirements and the design components in the application server that will ensure their fulfillment in a direct way (some other components that are indirectly needed to enforce some requirements are not directly mentioned in the list, but their role has been made clear through some comment) is shown:

* **R1**: The system must save the collected data of users registered to Data4Help in real time.
  + **DataCollectionManager:** this component manages to save the received data in the database in a correct way.
* **R2**: The system has to allow the third party that wants to retrieve some data to choose between an individual request or an aggregate one.
  + **RequestManager:** manages both individual and aggregate requests, it is able to distinguish the choice made by the third party on the ‘ThirdPartyWebApp’.
* **R3**: In case of a query for data of an individual the system has to ask to the third party the individual’s fiscal code.
  + **RequestManager:** contains the logic about individual requests, it retrieves the data of the right user thanks to his fiscal code. The fiscal code field is shown client’s side on the ‘ThirdPartyWebApp’.
* **R4**: In case of a query for aggregate data the system has to ask to the third party which parameters to use to filter data.
  + **RequestManager:** contains the logic about aggregate requests, it retrieves the correct data exploiting the filters provided. The filters are inserted client’s side on the ‘ThirdPartyWebApp’.
* **R5**: When a request for a specific individual’s data is made the system must allow the individual to accept the request or not.
  + **NotificationManager**: sends to the user a push notification with the informations about the request that has been made and that is provided by the ‘RequestManager’.
  + **ResponseManager**: handles the user’s answer allowing him to accept or refuse the request.
* **R6**: When a request for data is approved the system has to make the previously saved data available to the third party.
  + **RequestManager**: in case of a positive answer by the system (for both individual and aggregate requests), sends the data to the requesting third party.
* **R7**: The system must provide to the third party the possibility to subscribe to new data and receive them as soon as they are produced both for individuals and for groups of individuals.
  + **SubscriptionManager**: handles the subscription requests, the response of the interested user (in case of individual subscription) and it sends the new data as soon as they are produced (that are forwarded by the ‘DataCollectionManager’) to the third party that has done a successful subscription.
* **R8**: The system must allow the user to accept or refuse a possible request for subscription by a third party.
  + **ResponseManager**: it handles the user’s answer allowing him to accept or refuse the request of subscription.
  + **NotificationManager**: it sends to the user a push notification with the informations about the request of subscription that has been made (and forwarded by the ‘SubscriptionManager’).
* **R9**: The requests by third parties on aggregate data must provide them if and only if the number of individuals whose data satisfy the request is higher than 1000.
  + **RequestManager:** it contains the logic to make privacy controls on the requested data and provides them to the requesting third party if, and only if, the controls are passed.
* **R10**: When the number of users satisfying an aggregate request (for which a subscription was made) becomes less than 1000 the subscription is automatically canceled until the matching users become again more than or equal to 1000.
  + **SubscriptionManager:** it controls that the privacy controls are passed for subscriptions to data of groups of individuals and provides new data as soon as they are produced only in that case.
* **R11**: The system must allow the User to analyze its own data and stats providing him a way to access to all registered data and stats and giving him the possibility to consult both their aggregate (ex: daily average) values and precise measurements.
  + **UserDataVisualizationService:** provides the requested data and stats requested by the user.
* **R12**: The application on wearable devices, if AutomatedSOS is activated, must send the health parameters and location to the third party as soon as it detects that parameters are out of the defined bounds.
  + **SOSManager**: handles the SOS call and sends it to the ThirdParty providing the AutomatedSOS service that is closer to the user. The problem is detected client’s side: it is the ‘UserSmartwatchApp’ that has to analyze user’s data and control if they are in the defined bounds or not.
  + **NotificationManager**: it is concerned in sending the SOS message to the third party chosen by the ‘SOSManager’.
* **R13**: The system has to allow third parties that have activated the Track4Run service to schedule a run providing name, starting and ending point coordinates, the path, the date and time of the competition and the maximum number of participants.
  + **RunOrganizationManager**: handles the interaction with the third party that wills to organize a run competition.
* **R14**: The system has to allow users who have activated the Track4Run service to enroll for an organized run showing them the organized competitions on a calendar.
  + **EnrollmentManager**: handles the users’ requests of enrollment.
* **R15**: The system has to allow users who have activated the Track4Run service to follow the development of a run selecting an ongoing competition from a list that identifies runs by their name.
  + **RunWatchingManager**: contains all the business logic to allow users willing to watch a chosen competition to follow it on a map through their mobile application.

It is worth noting that in the provided mapping the ‘Router’ components are not mentioned for the sake of simplicity, but they are directly or indirectly connected to the fulfillment of the system functionalities because they route to the right component every message coming from the client’s side (except for the ones handled by the ‘ResponseManager’): the interfaces exposed by the application server are the ones provided by the three ‘Router’ components.