Politecnico di Milano

AA 2018-2019

POLITECNICO
MILANO 1863

Software Engineering 2

RASD

Requirements Analysis and Specification Document

11.11.2018

Table of Contents

1. Introduction

1.1 PURPOSE

Personal data, which include examples such as digital information on the position of users and their health, telephone call logs or web searches, are undoubtedly the oil of modern data-intensive science and the online economy, and are the basis for apps to provide intelligent services and personalized experiences to each user. The development of databases to manage them is therefore of fundamental importance.
In this context, TrackMe's DATA4Help is designed to be a Personal DataSpace Management System (PDSMS), i.e. not a real application for mobile devices, but a service at a lower level, at the base of possible future applications, such as AutomatedSOS, which this document will not deal with.
As a database, by registering in DATA4Help each user has the possibility to create a personal repository in which to store and handle his personal data, specifying the field of belonging and being able to count on the respect of his privacy, which must necessarily be guaranteed by this service. The first objective will be to allow third parties, also registered to the service, to apply for access to data of registered users, in order to monitor their location and health status.
Specifically, if a registered third party is interested to receive the data of a specific individual, a request will be made to TrackMe, which will pass it on to the user under consideration. In this regard, the user must have the opportunity to express his will and then to choose whether to share his data or not.
Similarly, a registered third party may also request TrackMe to receive anonymous data concerning groups (class) of individuals and in this case TrackMe will directly assess whether it is possible or not to make the requested data properly anonymous and then grant or not their transmission.

1.1.2 GOALS

[G1] DATA4Help allows users to be recognized by providing a method of identification

[G2] DATA4Help has to work as a Personal Dataspace Management System (PDSMS), in which each user is associated with a private repository in which to enter their personal data.

[G3] The user is guaranteed to have access at all times to his entered data, in order to monitor and possibly modify them.

[G4] Each user can express preferences that will be associated anto him and stored in his profile, such as the will to make his personal data not accessible or only partially accessible and to define certain third parties as not allowed or only partially allowed to access some data.

[G5] DATA4Help allows third party registration

[G6] Third parties can request specific data relating to a single individual

[G7] Third parties can request anonymous data relating to groups of individuals

[G8] The application must be able to allow individuals to express their will or not to make their data visible to third parties and must be able also to understand if certain data required, concerning groups of individuals, can be released or not

1.2 WORLD, SHARED AND MACHINE PHENOMENA

1.2.1 WORLD PHENOMENA

1. People use smartwatches or similar devices for their utilities

2. Each person is associated with personal data, such as data concerning his geographical location and his state of health

1.2.2 SHARED PHENOMENA

1. Each person can use his smartwatch in order to collect and eventually share his personal data with third parties.

2. Third Party may need data concerning a specific individual or a group of individuals and ask for them.

1.2.3 MACHINE PHENOMENA

1. Each user can create a Personal Data Space (PDS), that is a repository in wich to collect all his personal data

2. Each user can specify preferences in which to define which data are accessible and which are not and, where appropriate, to indicate particular third parties that do not have access to certain data

3. When a third party requests data relating to a specific user, TrackMe checks the preferences specified by that user and if the third party in question does not appear among those specified by the user as not allowed, passes the request to the user who can then accept it or reject it

4. If a third party requires data related to a group of individuals, TrackMe checks this class of users in an attempt to anonymize the requested data. If the number of users belonging to this class is less than 1000, the request is rejected 1.3 DEFINIZIONI, ACRONIMI, ABBREVIAZIONI

1.3 DEFINITIONS, ACRONYMS, ABBREVIATIONS

1.3.1 DEFINITIONS

- User (Data Owner): individual who, by choosing to access the DATA4Help service, accepts that TrackMe accesses his personal data, with the simultaneous creation of a repository associated to him that contains his own data and to which he can access at any time

- Data: all the informations concerning a single user, that the same user includes in his associated repository or also the informations related to a class of individuals. Data can belong to different fields, but for the purpose of this project, we consider for semplicity only two types of data, Health Data and Location Data.

- D4HPreferences: set of wills expressed by the user and associated to his account. Each user can define some data as not accessible and certain third parties as allowed or not allowed to access to some type of data.

- Repository (PDS): personal space containing all the data associated with a single user.

- Third Party (Data Demander): an external service, such as an application for smartphones or other devices, which is given the opportunity to use DATA4Help in order to access specific data concerning individuals, or anonymous data concerning groups of individuals

- QueryToSingleIndividuals: request by a third party of data concerning either a specific individual or a particular group of individuals, like those people that are over than 70 years old or people that live in a particular geographic area like Milan.

1.3.2. ACRONYMS

- RASD: Requirement Analysis and Specification Document
- API: Application Programming Interface
- PDS: Personal Data Space
- PDSMS: Personal DataSpace Management System

1.3.3. ABBREVIATIONS

- [Gn]: n-th goal
- [Dn]: n-th domain assumption
- [Rn]: n-th functional requirement

2. Overall Description

2.1 PRODUCT PERSPECTIVE

As already mentioned above, DATA4Help is a service to be understood as a PDSMS, in which each of the users who is registered, become associated with a repository, i.e. a private space containing his personal data. A third party may have access to this service, requesting informations about a single individual or a group of individuals and awaiting a response regarding the possibility or not to allow data transmission. To better understand the structure of the domain model, the following class diagram is shown:

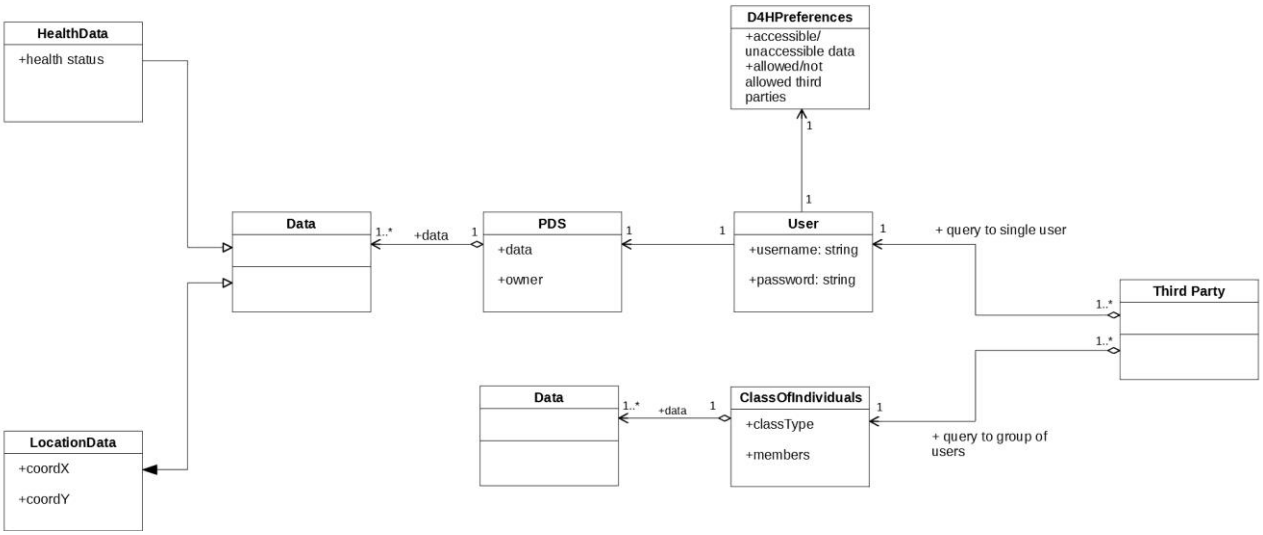


Figura 1: Class Diagram

In addition is defined below a state diagram that rappresents graphically either the request, made by a third party, to a single individual or to a group of individuals:

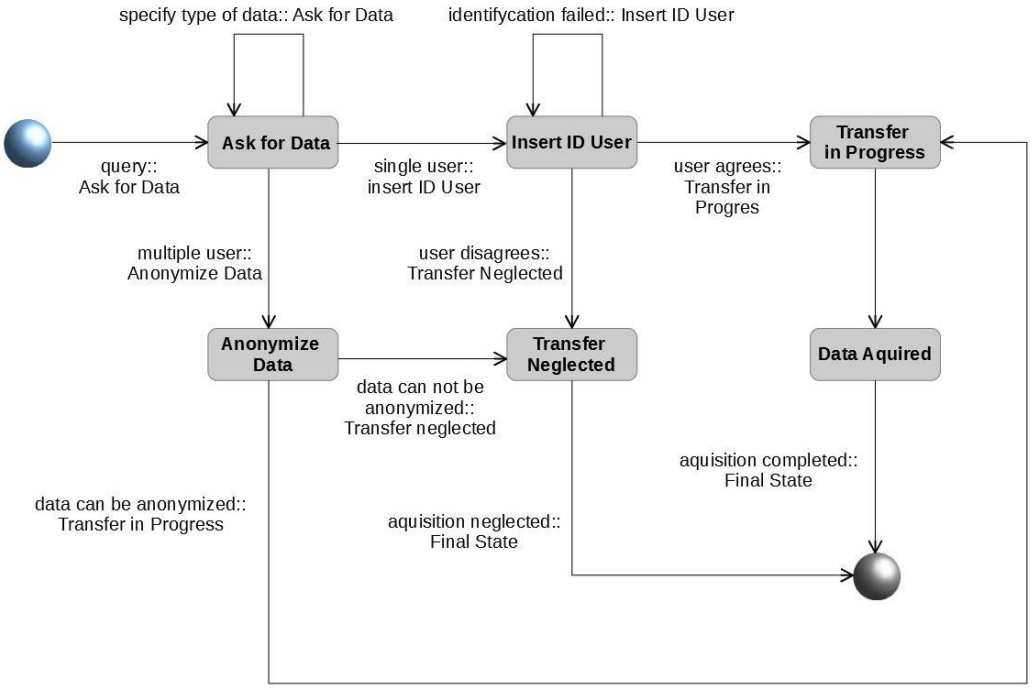


Figura 2: State Diagram

In this diagram all possible situations arising from the third party's request have been taken into account and therefore represented. In particular, in defining the portion of the diagram relating to the request for data concerning a single individual, it was assumed that the third party applicant is in possession of an identifier of the individual, such as a security number or a fiscal code in the italian case, to be provided to DATA4Help in order to search for the PDS associated.

2.2 PRODUCT FUNCTIONS

Referring to the goals reported in section 1.1.2, it is easy to see that the main functions that this service must ensure are essentially 3, listed below:

- Personal Data Acquisition and Storing
- Preference Management
- Data Sharing Control

In the following sections these functions will be reviewed and analysed in more detail.

2.2.1 Personal Data Acquisition and Storing

As specified in [G2] and [G3], DATA4Help must work as a Personal DataSpace Management System, that is as a sort of online store where the data providers publish their valuable data and the data demanders subscribe or query data on demand. As a virtual space in which the supplydemand forces and the exchange of information co-exist. A repository is then set up for each user who registers for this service, to act as a storage space for personal information, ensuring that this information will not be lost and that will be accessible to the his owner in any time. Personal data, the digital record of "everything a person makes and does online or in the real-world", encompasses digital identity; relationships to other people and organizations; real-world and online context, activity, interests and behavior; communications data and logs; media produced;consumed and shared; financial data; health data and institutional data. In the specific case of DATA4Help, the most relevant data are the location and the state of health of the individual.

2.2.2 Preference Management

DATA4Help should not only be responsible for the data storage, data analysis, data pricing, more importantly, for ensuring data privacy and security, while ensuring data control, transparency and confidentiality. As already defined in [G7], each individual, by registering for the service and becoming an associated user, has the opportunity to express preferences regarding the visibility of their personal data. Specifically, the user may express the wish to render unaccessible all his data to any third parties, or define only certain data as accessible. It may also be possible for the user to define certain third parties as not allowed to access to any data or to only certain data. DATA4Help must therefore provide a space in which these preferences are stored and must ensure, from the moment of their definition onwards, that these preferences will be observed and respected, in accordance with the wishes of the user.

2.2.3 Data Sharing Control

The main operation DATA4Help has to guarantee is data sharing, i. e. providing the possibility for third parties to register and request the acquisition of data concerning specificindividuals or groups of individuals. In the first case, once the request is made and have been recognized within DATA4Help the profile associated with the user whose data the third party wants to acquire, TrackMe itself must first consult the preferences defined by the user interested by the request and deny access to data if the case study does not conform to what is specified in the same preferences, or allow access and then start the transaction if the user agrees. In the latter case, TrackMe will directly determine whether the transaction is possible or not, basing the decision on whether or not is possible to anonyze data required.

2.3 USER CHARACTERISTICS

The actors who are supposed to be the users of this service are exentially the sequent:

- User

A single individual that is succesfully registered to DATA4Help and has an associated repository that he manage in any time. In the domain of a data market he is a data owner who has the total control of hi own data.

- Third Party

An external service, such as an application for smartphones or other devices, which is given the opportunity to use DATA4Help in order to access specific data concerning individuals, or anonymous data concerning groups of individuals

2.4 DOMAIN ASSUMPTIONS

[D1] User's login credentials are unique within the system

[D2] Each repository stored in DATA4Help refers to no more than one user

[D3] Acquisition of an individual's personal data may be made through smartwatches, smartphones or other devices owned by the same individual

[D4] Each individual is associated with an identifier, such as security number, identity card or fiscal code in the italian case, which distinguishes him and which can then allow both TrackMe and third parties to identify him.

[D5] There is a reliable Internet connection that allows access to use TrackMe app or to TrackMe website

3. Specific Requirements

3.1 EXTERNAL INTERFACE REQUIREMENTS

3.1.1 USER INTERFACES

The following project does not define an actual visual implentation of a user interface for Data4Help service. Anyway, possible ideas to define the structure of this type of interface are reported. As mentioned before, the main idea of this project is that TrackMe is seen as a mobile application, available in an App Store and accessible to any user. In this vision DATA4Help is an internal serive offered by TrackMe that works like a Data Space Management System.
Once downloaded from the digital store, the user will be able to run TrackMe, that will first ask the him to provide his personal credentials to log in or otherwise, if the user has not yet been registered, to register for the service.
In order to do this, the user will be shown a first screen in wich there will be a section of Log in, with associated fields in which to enter Username and Password, and a section for the Sign Up, for the registration of new users.
When a user wants to be registered on TrackMe, he only has to select the Sign Up section. At this point, the user will be asked to provide his security number or his fiscal code, a username of his choice and a password that respects the security fees imposed by the system. Once provided valid credentials, the user will be directed to a new window where he can express his willingness in order to allow TrackMe to create a repositorystored in DATA4Help, containing his personal data, thereby accepting that these will be acquired by the system.
Once this procedure has been completed, the user is correctly authenticated and is then directed to the screen corresponding to his TrackMe profile. Specifically, a notification section will be set up, in order to allow the user to view possible reports of requests for data access by third parties. There will be also a preference section, called D4HPreferences, where the user will have the possibility to define certain data as not accessible and also to designate specific third parties as not allowed to access some specific data.

3.1.2 HARDWARE INTERFACES

DATA4Help is supposed to be a PDSP and an internal service powered by Trackme, wich is meant to be a software application, and as a database, DATA4Help has the main function to collect and manage personal data, allowing also their transmission to third parties, according to the volunties expressed by data owners. It is not using any hardware interfaces but certainly it requires using a smartphone with an internet connection to run TrackMe app or a personal computer within a web browser in order to reach TrackMe website. This devices are also necessary to allow data acquisition by DATA4Help in order to properly create Personal Data Spaces, and for this purpose also smarthwatches can be used.

3.1.3 COMMUNICATIONS INTERFACES

Searching among the documents proposed in the literature has emerged a project, called openPDS [1][2], which in building a DSMS defines a new system called SafeAnswers, to be integrated into the database in order to ensure greater security when external entities access to personal data. Therefore it is possible to use the same tool for the development of DATA4Help and in particular the system may be composed by meta-PDS and groupPDS.

The meta-PDS refers to the personal data set, as shown in Figure 3, and the information accessing procedure is as follows:

1) The request of the data demander is sent to SA module.

2) SA module access the internal database to finish the related computation.

3) The data demander get the result through the SA module.

It is clear that the SA module shields the internal database and the demander, also accomplishes access audit and control.
Group-PDS, composing of multiple meta-PDS, protect privacy through secure multi-party computation, as shown in Figure 4:

1) The Service release data requirements.

2) Information exchange and computation (for example, the security multi-party computation) among individual meta-PDS.

3) Group-PDS returns query results.

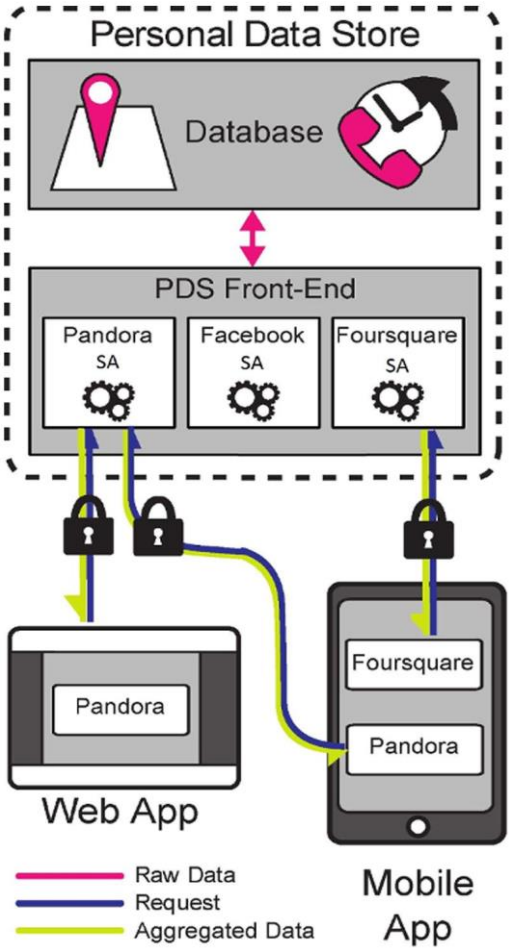


Figura 3: meta PDS

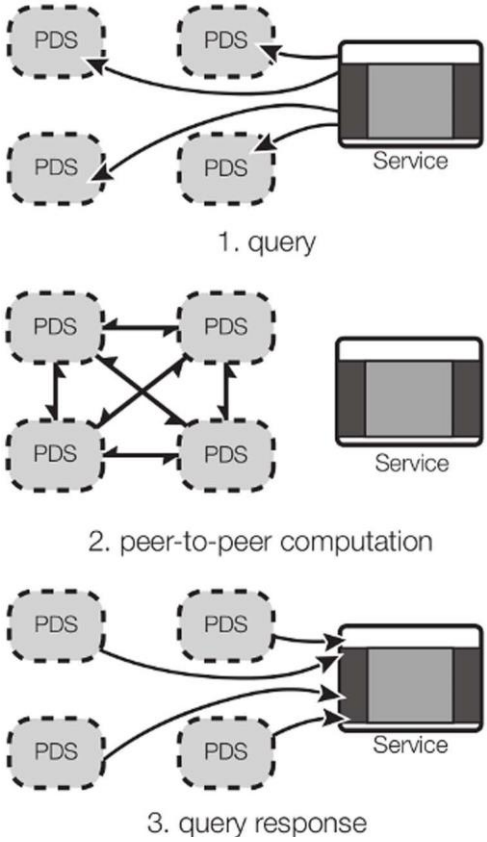


Figura 4: group PDS

3.2 FUNCTIONAL REQUIREMENTS

[G1] DATA4Help allows users to be recognized by providing a method of identification

[D1] The user's login credentials are unique within the system

[R1] The user can create an account for the usage of TrackMe, by selecting a username and a password. The username must not be already taken by any other user and the password must respect the security rules imposed by the system.

[G2] DATA4Help has to work as a Personal Dataspace Management System (PDSMS), in which each user is associated with a private repository in which to enter their personal data.

[D2] Each repository stored in DATA4Help refers to no more than one user

[D3] Acquisition of an individual's personal data may happen through smartwatches, smartphones or other devices owned by the same individual

[R2] By only providing the credentials that have been defined during the registration, the user is allowed to create ad manage his associated repository in DATA4Help

[R3] A single user can not have access to another user's repository

[G3] All'utente è garantito di avere accesso in ogni momento ai propri dati inseriti, al fine di monitorarli ed eventualmente modificarli

[R4] L'utente, by providing an email address, può recuperare le credenziali di accesso nel caso le perda o non sia in grado di inserirle

[R5] Any action or change that a user makes on their PDS is stored and can not be lost

[G4] Each user can express preferences that will be associated anto him and stored in his profile, such as the will to make his personal data not accessible or only partially accessible and to define certain third parties as not allowed or only partially allowed to access some data.

[R6] A set of preferences cannot be associated with more than one user.

[R7] Only one set of preferences can be associated to each user.

[G6] Third parties can request specific data relating to a single individual

[D4] Each individual is associated with an identifier, such as security number, identity card or fiscal code in the italian case, which distinguishes him and which can then allow both TrackMe and third parties to identify him.

[R8] A third party must provide a valid identifier associated with the user from whom it wants to receive the data and explicitly declare to the service what data specifically is to be obtained.

[R9] When a third party requests to access the data of a single user, TrackMe checks the preferences defined by the user, stored in his associated PDS. If TrackMe finds that the user have declared in his preferences the will not to allow access to any data, or that the data requested by the third party do not fall within the data defined in the user'preferences as accessible, or that the third party is not allowed to access that particular type of data, TrackMe will immediately notify the third party that it is impossible to access data, by sending an appropriate Warning. Otherwise, TrackMe will send a communication to the, who may then give his consens or not, and then communicate the outcome to the third party.

[G7] Third parties can request anonymous data relating to a group (class) of individuals

[R10] The third party must specify the class type and what data it wants to obtain by it.

[R11] Requests for anonymous data relating to groups of individuals are handled directly by TrackMe, which must check whether these data can be anonymized or not. If TrackMe can not anonymize those data, the transmission is not allowed.

[R12] If the number of members of the class whose data are requested is less than 1000, TrackMe notifies the requesting third party that it is unable to allow the transmission, by sending it a Warning.

[R13] If the number of members of the class exceeds 1000, TrackMe collects the required data within DATA4Help and sends it to the third party, with a notification of transmission.

3.2.1 USE CASE DIAGRAM

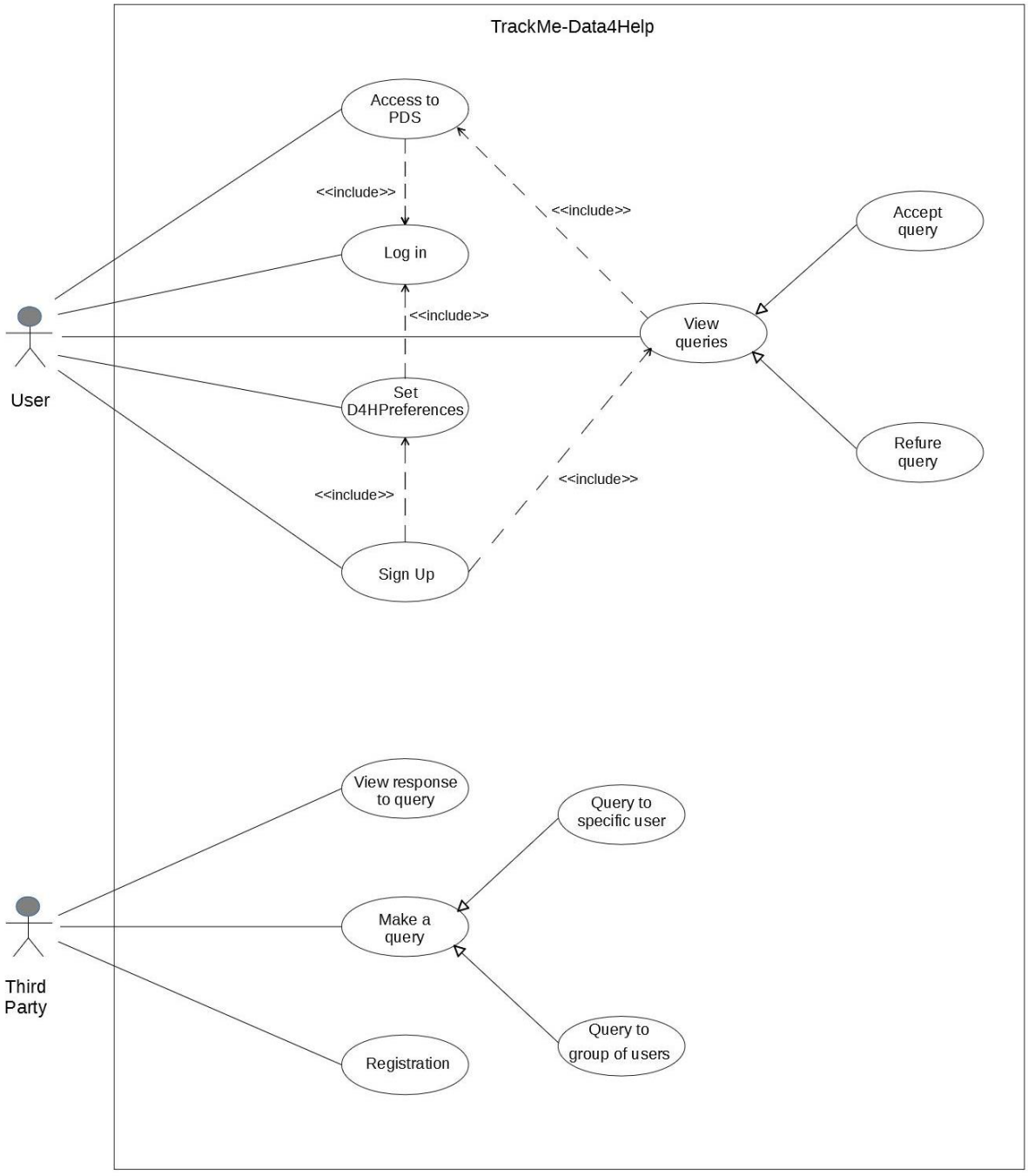


Figura 4: Use Case Diagram

Name	Sign Up
Actor	User
Entry conditions	The user has installed the TrackMe application on his/her device or has accessed to TrackMe website.
Events Flow	1. Click on “Sign up” button 2. Provide all the necessary information to create an account, like a valid email address, a password, a security number or a fiscal code ad a Username 3. Cilck on “Create a personal PSD in DATA4Help” 4. Agree that TrackMe’ll acquire all the personal data 5. Click on “Confirm” button 6. The system saves the data
Exit Conditions	A TrackMe account has been succesfully created, with also an associated personal data space registered in DATA4Help
Exceptions	1. The user is already signed up 2. The user didn’t fill all of the mandatory fields with valid data 3. The username is already taken 4. The e-mail is already registered 5. All the exceptions are handled by notifying the user and taking him back to the sign up activity.

Name	Log in
Actor	User
Entry conditions	The user has properly registered a TrackMe account associated to him
Events Flow	1. The User provide the credentials that he has defined during the sign up, like a “Username” and an associated “password” 2. Click on “Access” button
Exit Conditions	The User can access to his TrackMe account
Exceptions	1. The user enters invalid Username 2. The user enters invalid Password 3. All the exceptions are handled by notifying the user and taking him/her back to the login activity

Name	Set DATA4Help Preferences
Actor	User

Entry conditions	The user has already logged in
Events Flow	1. The user chooses setting general preferencies 2. The user specifies to set his/her DATA4Help preferences 3. The user specifies if he wishes not to make any data visible to third parties or to make only certain types of data visible. He also specify if there are some third parties who can not access to some specific data 4. The system saves the preferencies
Exit Conditions	The preferences specified by the user are properly registered in his account, and will be respected by the system in order to garatee privacy
Exceptions	/

Name	View queries
Actor	User
Entry conditions	The user has already logged in
Events Flow	1. The user accesses the newsletter prepared in his personal account 2. The user check if there are some queries concerning his PSD
Exit Conditions	The user has checked all the notifications sent to his profile, including notices regarding requests coming from third parties for access to his personal data
Exceptions	/

Name	Accept query
Actor	User
Entry conditions	The user has already viewed some queries in his newsletter
Events Flow	1. The user answers to the request by writing a message 2. The user allows the third party to access the data requested 3. TrackMe takes the message provided by the user and sends it to he third party
Exit Conditions	TrackMe provides the trasmission of user's personal data to the third party, respecting the wishes of the user
Exceptions	1. TrakMe fails sending the message to the third party due to problems with the internet connection 2. The data transmission fails within DATA4Help

Name	Refuse query
Actor	User
Entry conditions	The user has already viewed some queries in his newsletter
Events Flow	1. The user answers to the request by writing a message 2. The user doesn't allow the third party to access the data requested 3. TrackMe takes the message provided by the user and sends it to he third party
Exit Conditions	TrackMe informs the third party that the user hasn't allowed his data transmission, so the transmission doesn't take place
Exceptions	1. TrakMe fails sending the message to the third party due to problems with the internet connection

Name	Registration
Actor	Third Party
Entry conditions	The third party has already accessed to TrackMe website or to TrackMe applications
Events Flow	1. The third party accesses a specific field dedicated to external bodies, distinct from the registration field dedicated to normal users 2. The third party provides all the necessary information in order to identify itsels as an allowed external service 3. The system saves the data
Exit Conditions	The third part is correctly registered to TrackMe and can take advantage of the services offered by it, including the possibility of logging in to DATA4Help and requesting access to data concerning specific individuals or groups of individuals
Exceptions	1. The third party is already registered 2. The third party didn't fill all of the mandatory fields with valid data 3. All the exceptions are handled by notifying the third party and taking it back to the registration activity.

Name	Make a query/ Query to specific User
Actor	Third Party

Entry conditions	The third part has already been correctly registered
Events Flow	1. The third party access to a specific field in wich it is possible to send some requests to TrackMe 2. The third party express the particular wish to access some data of specific individual through DATA4Help 3. The third party provides an identifier of the user from whom certain data would be obtained 4. The third party specifies what data to request from user's PSD
Exit Conditions	All the details specified by the third party have been collected by TrackMe, which immediately sends an alert to the user
Exceptions	1. By checking the "DATA4Help preferences" expressed by the user from which the third party would like to obtain certain data, TrackMe has verified that such requested data can not be transmitted to the third party 2. The indentifier provided by the third party doesn't refer to any user 3. The user from whom certain data would be obtained has no longer an associaed trackMe account 4. TrakMe fails sending the alert to the user due to problems with the internet connection 5. All the exceptions are handled by notifying the third party and taking it back to making queries activity.

Name	Make a query/ Query to group of Users
Actor	Third Party
Entry conditions	The third part has already been correctly registered
Events Flow	1. The third party access to a specific field in wich it is possible to send some requests to TrackMe 2. The third party express the particular wish to access some anonymized data of groups of individuals through DATA4Help 3. The third party defines what type of group or class of individuals it iss interest about 4. The third party specifies what data to request from DATA4Help
Exit Conditions	This type of query is properly received and directly handled by TrackMe that approves it if it is able to properly anonymize the requested data
Exceptions	1. TrakMe fails to receive the request due to problems with the internet connection 2. TrackMe finds that the number of individuals whose data satisfy the request is lower than 1000, so it can not accept that request 3. All the exceptions are handled by notifying the third party and taking it back to making queries activity.

Name	View responses to queries
Actor	Third Party
Entry conditions	The third part has already been correctly registered
Events Flow	1. The third party access to a specific field in wich it is possible to send some requests to TrackMe 2. The third party express the particular wish to access some data of specific individual through DATA4Help 3. The third party provides an identifier of the user from whom certain data would be obtained 4. The third party specifies what data to request from user's PSD
Exit Conditions	All the details specified by the third party have been collected by TrackMe, which immediately sends an alert to the user
Exceptions	1. By checking the "DATA4Help preferences" expressed by the user from which the third party would like to obtain certain data, TrackMe has verified that such requested data can not be transmitted to the third party 2. The indentifier provided by the third party doesn't refer to any user 3. The user from whom certain data would be obtained has no longer an associaed trackMe account 4. TrakMe fails sending the alert to the user due to problems with the internet connection 5. All the exceptions are handled by notifying the third party and taking it back to making queries activity.

3.2.2 SEQUENCE DIAGRAMS

Following is reported a sequence diagram that describes the process that represents the principal objective of the service DATA4Help offered by TrackMe, that is the possibility for third parties to demand relative data both single individuals and groups of individuals. Specifically, the diagram below describes the request for access to personal data concerning a specific individual registered with DATA4Help:

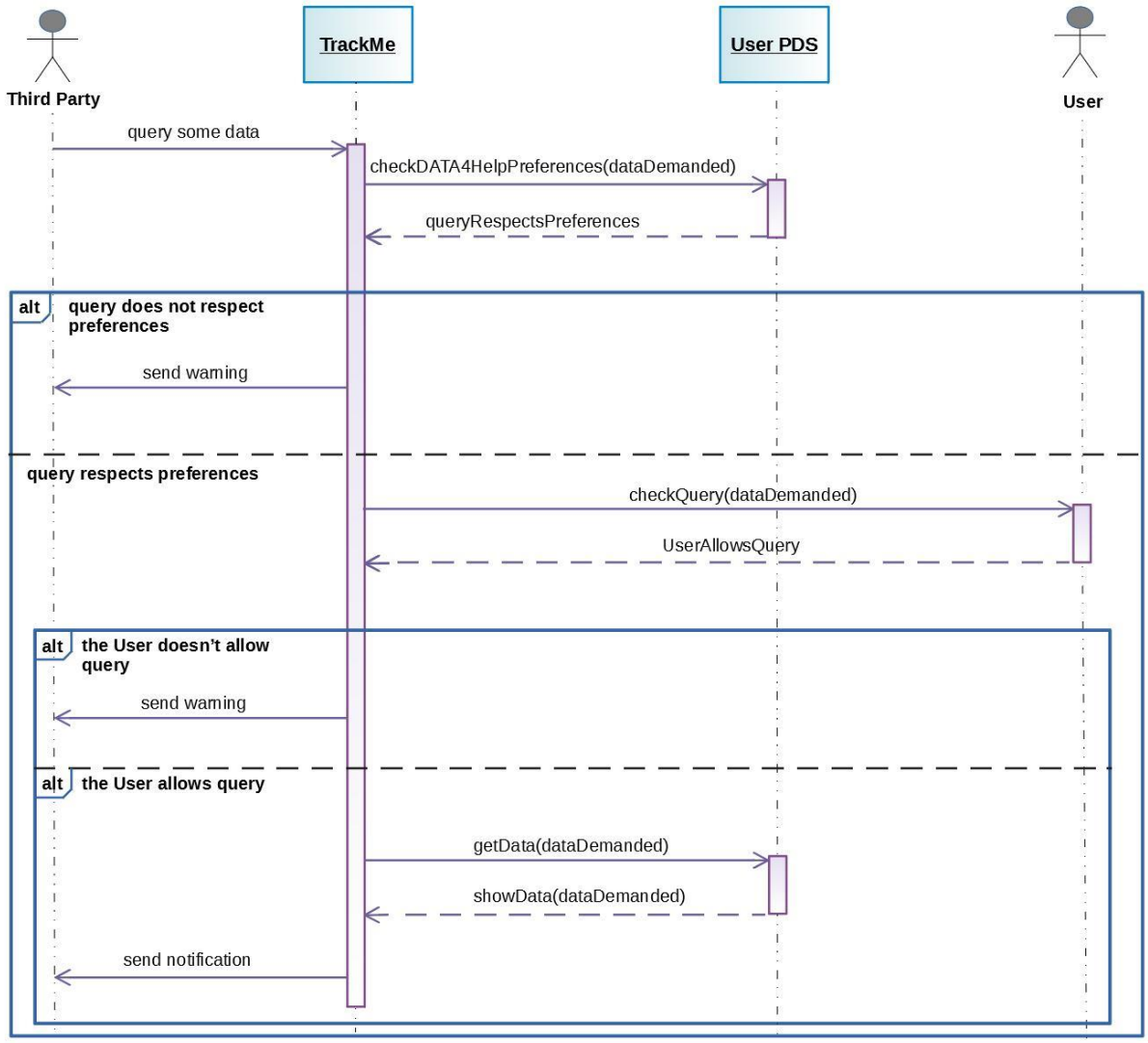


Figura 5: Sequence Diagram

Where "User PDS" identifies the DATA4Help repository that contains all personal informations associated to the user.

3.3 PERFORMANCE REQUIREMENTS

DATA4Help, as a Data Space Management System, must be able to serve fairly great numbers of users simultaneously. In particular, it is required that this system is able to manage many repositories, each one associated with a single user, while ensuring data privacy.
The data available from the participants is heterogeneous and dynamic. Accessing it requires support for multiple Web APIs, formats, and protocols, as well as high tolerance to errors and unknowns.
This service must have available all the information required to be able to access the data in all the participating data sources, thus relying on the identity management and cataloging services.
When a third party requests data relating to a single user, DATA4Help has to recognize the PDS associated to that user, check the set of preferences saved into it, access to data required and provide the transmission of them to the third party. By focusing on accessing data contained in a specific repository, the user must be guaraneed whether or not to allow access to the requested data, while preventing only the requested data from being transmitte.
Other requirements that this system must guarantee as its own, are the ability to make anonymous information about classes of people and to protect the data against all the apps that deliberately try to infer sensitive information by over-querying a user's PDS or by colluding with other apps.

3.4 DESIGN CONSTRAITS

3.4.1. HARDWARE LIMITATIONS

As already mentioned in section 3.1.2, this project aims to propose the development of a TrackMe application, of which DATA4Help is an internal service among the various available and the only on which we are focused, so it does not provide for hardware interfaces or even less hardware limitations. As an application or a web site, all you need is a smartphone from which you can download and use the TrackMe app or a PC from which you can access the web site associated with TrackMe. Of course, it will also be necessary to have an adequate internet connection.

4. Formal Analysis Using Alloy

In this section, the Alloy model is given. In the definition of the model, all the system constraints defined in the previous sections are declared and respected. More precisely, the main constraints that have been made valid for the system are as follows:

- a data belonging to a user cannot be owned by another user at the same time, as it is a personal data related to a specific individual.

- Each user can define a single set of preferences regarding the access of their data and same set of preferences can not be associated with two distinct individuals.

- When a third party requests access to the data of an individual, before transmitting the notification to the user, TrackMe checks the preferences expressed by him and in case it already emerges from these that the transmission is not feasible, no report is sent to the user concerned, while a Warning is sent to the requestig third party.

- If the preferences expressed by the user do not reveal any impediment to trensmission, TrackMe notifies the user of the reguest by sending him a notification. The user can now decide for himself whther or not to allow the transmission of his data.

- If a third party requests data about a group (class) of individuals, TrackMe allows access to such data only if possible to anonymize them, that is, for semplicity, if the number of class members is greater than 1000. However, for semplicity, in the deefinition of this model has been used a threshold of 2 instead of 1000 (this simplification would certainly not lead to a secure system for the privacy of users in reality, but has been placed exclusively to treat the problem more easily).

4.1 ALLOY MODEL

```
open util/integer
abstract sig  Bool {}
sig True extends Bool{}
sig False extends Bool{}


sig ThirdParty {
	queriesToIndividuals: set QueryToSingleUser,
	queriesToGroup: set QueryToGroupOfUsers,
}


sig QueryToGroupOfUsers{
	mittent: one ThirdParty,
	receivers: one Class,
	dataDemanded: set Data,
	--warnings: set ImpossibleToAnonimyzeDataWarning,
	accepted: one Bool
}

--a query by a ThirdParty in order to access some data
sig QueryToSingleUser {
	mittent:one ThirdParty,
	dataDemanded: set Data,
	receiver: one User,
	accepted: one Bool,
	--warnings: set UnaccessibleDataWarning
}
sig Class {
	members: set User,
	classType: one ClassType
}


abstract sig ClassType{}
one sig Over70People extends ClassType{}
--one sig ResidentInMilanPeople extends ClassType{}


sig User {
	personalData: set Data,
	preferences: one D4HPreferences,
	notifications: set UserNotification,
	receivedQueries: set QueryToSingleUser
```

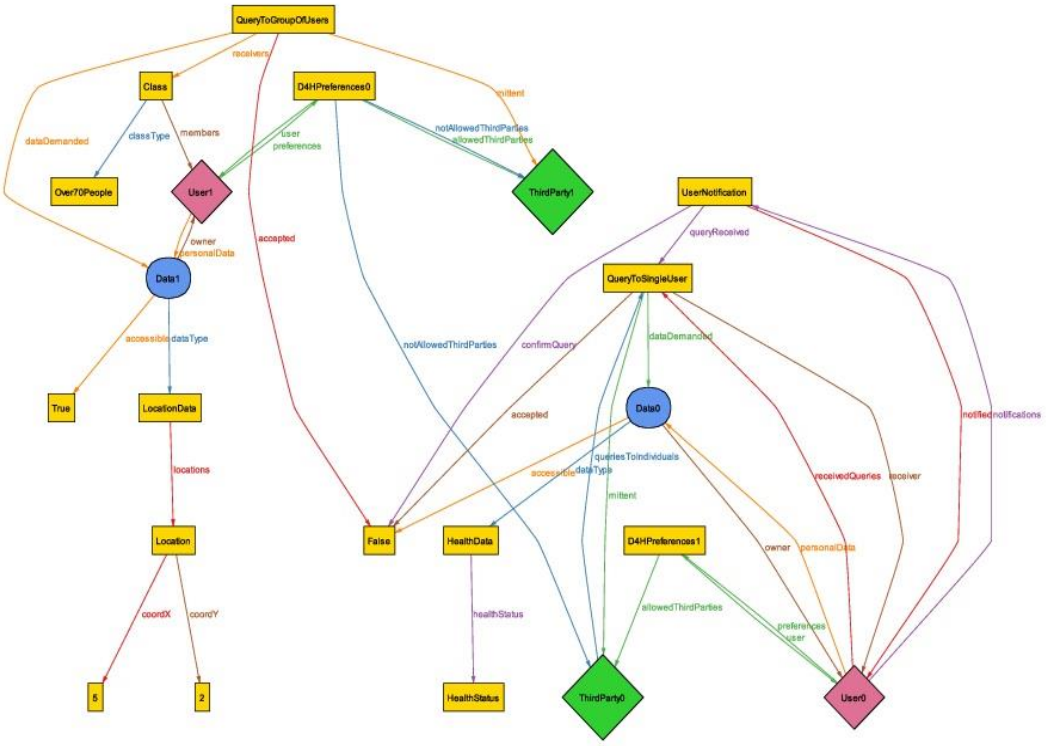
```
abstract sig Data {
        owner: one User,
        dataType: one DataType,
        accessible: one Bool
}


sig DataType{}
sig HealthData extends DataType {
        healthStatus: one HealthStatus
}
sig LocationData extends DataType {
        locations: one  Location
}


sig Location {
        -- latitude
        coordX: one Int,
         -- longitude
        coordY: one Int
}

sig  HealthStatus{}

--notification reaches a User, when a ThirdParty asks for his data
sig UserNotification {
        notified: one User,
        queryReceived: one QueryToSingleUser,
        confirmQuery: one Bool
}



sig D4HPreferences {
        user: one User,
        --data defined by the User as accessible by third parties
        accessibleData: set Data,
        --data defined by the User as not accessible by any third party
        unaccessibleData: set Data,
        --third parties which the User defines as allowed to access some data
        allowedThirdParties: set ThirdParty,
        --third parties which the User defines as not allowed to access some data
        notAllowedThirdParties: set ThirdParty
}
```

```
fact DataUserConnection {
	all  u: User | all  d: Data | ( d in u.personalData implies  d.owner = u) and
	(d.owner = u implies  d in u.personalData)
}


fact NoTwoUsersToTheSameData {
	all d1: Data | no disj u1,u2:User | d1.owner= u1 and d1.owner= u2
}


fact UserPreferencesConnection {
	all u1: User | all p1: D4HPreferences | ( u1.preferences= p1 implies p1.user = u1) and
	(p1.user= u1 implies u1.preferences= p1)
}


fact NoTwoUserToSamePreferences {
	all p1: D4HPreferences | no disj u1, u2: User | u1.preferences=p1 and u2.preferences=p1
}


fact NoTwoPreferencesToSameUser {
	all u1: User | no disj p1, p2: D4HPreferences | p1.user= u1 and p2.user=u1
}


fact DataAccessibleD4HPreferencesConnection {
	all u1:User | all p1: D4HPreferences | all d1: Data | (p1= u1.preferences and d1 in p1.accessibleData) implies
	(d1 in u1.personalData and d1.accessible=True)
}



fact DataUnaccessibleD4HPreferencesConnection {
	all u1:User | all p1: D4HPreferences | all d1: Data | (p1= u1.preferences and d1 in p1.unaccessibleData) implies
	(d1 in u1.personalData and d1.accessible=False)
}

--each data defined in a D4HPreferences setting can not be owned by two different users,
--because each set of preferences refers to only one user and only to his data
fact DataInPreferencesReferToOnlyOneUser{
	all p1: D4HPreferences| all d1: Data| no disj u1,u2: User |
	(d1 in p1.accessibleData and d1 in u1.personalData and d1 in u2.personalData)
	or
	(d1 in p1.unaccessibleData and d1 in u1.personalData and d1 in u2.personalData)
}


fact QueryToSingleUserUserConnection {
	all u1: User | all q1:QueryToSingleUser | (q1.receiver = u1 implies q1 in u1.receivedQueries) and
	(q1 in u1.receivedQueries implies q1.receiver=u1)
}
```

```
fact UnacceptedQueryToSingleUser {
	all q1: QueryToSingleUser | q1.accepted = False iff
	(q1.dataDemanded in q1.receiver.preferences.unaccessibleData or
	q1.mittent in q1.receiver.preferences.notAllowedThirdParties or
	(some n1: UserNotification | n1.notified= q1.receiver and n1.queryReceived= q1 and n1.confirmQuery = False))
}


fact AcceptedQueryToSingleUser{
	all q1: QueryToSingleUser | q1.accepted = True iff
	(q1.dataDemanded in q1.receiver.preferences.accessibleData and
	(some n1: UserNotification | n1.notified= q1.receiver and n1.queryReceived= q1 and n1.confirmQuery = True))
}

fact AcceptedQueryToGroupOfUsers {
	all q1: QueryToGroupOfUsers| q1.accepted=True iff (#q1.receivers.members>1000)
}


fact UnacceptedQueryToGroupOfUsers {
	all q1: QueryToGroupOfUsers| q1.accepted=False iff (#q1.receivers.members<=1000)
}


fact DataAccessibleAnNotAccessibleAtTheSameTime {
	all p1: D4HPreferences |no d1: Data |  ((d1 in p1.accessibleData) and (d1 in p1.unaccessibleData))
}


fact QueryToSingleUserGenerateUserNotification {
	all q1: QueryToSingleUser | all u1:User | u1= q1.receiver implies
	 (one n1: UserNotification| n1.notified = u1 and n1.queryReceived = q1 and q1.accepted=n1.confirmQuery)
}


fact NotificationUserConnection {
	all u1: User | all n1: UserNotification | (n1.notified = u1 implies n1 in u1.notifications) and
	(n1 in u1.notifications implies n1.notified=u1)
}


--if a third party makes a query to a single user,the query is not about data concerning another user
fact DataDemandedInQueryToSingleUserAreOwnedByTheSameUserWhoReceivesQuery{
	no q1: QueryToSingleUser | q1.dataDemanded.owner != q1.receiver
}
```

```
--if a third party makes a query to a class of users,the query is about data concerning only the data
--about users who are members of this class
fact DataDemandedInQueryToGroupOfUsersAreOwnedByGroupMembers{
	all q1: QueryToGroupOfUsers | no d1:Data | (d1 in q1.dataDemanded) and (d1.owner !in q1.receivers.members)
}


pred show () {
	one d1:Data | d1.dataType = HealthData and (one d2:Data | d2.dataType = LocationData)
	one d1:Data | d1.accessible = True and (one d2:Data | d2.accessible= False)
	one t1: ThirdParty | #t1.queriesToIndividuals=1 and #t1.queriesToGroup=0
	one c1: Class | one u1: User | one q1: QueryToSingleUser| c1.members=u1 and q1.receiver!=u1
}
--run show for 1 but 2 User, 2 Data, 2 DataType, 2 D4HPreferences
run show for 2 but 1 QueryToGroupOfUsers, 1 QueryToSingleUser, 1 Class, 1 ClassType, 1 Location,1 HealthStatus, 1 UserNotification
```

4.2 WORLD OBTAINED BY THE ALLOY MODEL



5. REFERENCES

[1] Slides - "World and Machine.pdf"

[2] Slides - "UML for Requirements Engineering.pdf"

[3] The Unified Model Language (https://www.uml-diagrams.org/)

[4] De Montjoye Y-A, Shmueli E, Wang SS, Pentland AS (2014) openPDS: *Protecting the Privacy of Metadata through SafeAnswers*. PLoS ONE 9(7): e98790. doi:10.1371/journal.pone.0098790

[5] Xiangqian Dong, Bing Guo, Xuliang Duan, Yuncheng Shen, Hong Zhang, ,DSPM: *A Platform for Personal Data Share and Privacy Protect Based on Metadata*, College of Computer Science Sichuan University Chengdu, China

[6] Laura Dragan, Markus Luczak-Roesch, and Nigel Shadbolt: *Understanding Personal Data as a Space - Learning from Dataspaces to Create Linked Personal Data*, University of Southampton, UK

[7] Slides - "Usage of alloy in RE.pdf"

[8] A Guide to Alloy(https://www.doc.ic.ac.uk/project/examples/2007/271j/suprema_on_alloy/Web/tutorial0.php)