Specific Targeted Research Projects (STReP)

SocIoTal

Creating a socially aware citizen-centric Internet of Things

FP7 Contract Number: 609112

D5.1 –Trial and pilot specifications

Deliverable report

Contractual date of delivery:	30/11/2014
Actual submission date:	23/12/2014

Deliverable ID:	D5.1
Deliverable Title:	Trial and pilot specifications
Responsible beneficiary:	DNET

Contributing beneficiaries:	DNET, RD, UC, UMU, SAN, NS.
Estimated Indicative Person Months:	12

Start Date of the Project: 1 September 2013 Duration: 36 Months

Revision: 1

Dissemination Level: Public

Document Information

Document ID:	SOCIOTAL_D5.1_Trial_and_pilot_specifications_FINAL
Version:	Final 1.0
Version Date:	17 December 2014
Authors:	Nenad Gligoric, Dejan Drajic, Mirjana Nikolic, Srdjan Krco (DNET), Carmen Lopez, Ignacio Elicegui Maestro, Luis Muñoz, Luis Sánchez (UC), Michele Nati, Dionysia Triantafyllopoulou, Klaus Moessner (UNIS), Jorge Bernal, J.Luis Hernandez, Antonio Skarmeta (UMU),
Security:	**Public**

Approvals

	Name	Organization	Date	Visa
Project Management Team	Klaus MOESSNER	UNIS	28/02/2014	

Document history

Revision	Date	Modification	Authors
Draft	02/06/2014	First TOC draft	DNET/UC
Draft	31/07/2014	Initial TOC modification	UC
Draft	17/10/2014	Section 2.5 and 2.6 added	DNET
Draft	23/10/2014	Added sections 2.7 2.8 2.9	UNIS
Draft	26.10.2014	3.3.2 section added	DNET
Draft	31/10/2014	Section 2.5.2.1 and 2.6.2.1 with KPI updated	DNET
Draft	03/11/2014	Comments and minor revision of the document	UC
Draft	05/11/2014	Sections 2.7 2.8 2.9	UNIS
Draft	19/11/2014	Use cases in Section 2.5 and 2.6 updated	DNET
Review Release	14/11/2014	First release to be reviewed	RD
Draft	21/11/2014	Updated contribution from UMU	
Final Release	17/12/2014	Final revision	ALL
Final Version	23/12/2014	Final version ready for submission	DNET

Content

List of Figures

List of Tables

Section 1 - Introduction

1.1 SocIoTal purpose (DNET)

SocIoTal addresses a crucial next step in the transformation of an emerging business driven Internet of Things (IoT) infrastructure into an all-inclusive one for the society by accelerating the creation of a socially aware citizen-centric Internet of Things. It will close the emerging gap between business centric IoT enterprise systems and citizen provided infrastructure. SocIoTal will establish an IoT eco-system that puts trust, user control and transparency at its heart in order to gain the confidence of everyday users and citizens. By providing adequate socially aware tools and mechanisms that simplify complexity and lower the barriers of entry it will encourage citizen participation in the Internet of Things. This will add a novel and rich dimension to the emerging IoT ecosystem, providing a wealth of opportunities for the creation of new services and applications that address true societal needs and allow the improvement of the quality of life across European cities and communities.

1.2 WP5 Objectives (DNET)

The main goal of this WP is to design, deploy and coordinate two pilot services, so as to assess the feasibility and applicability of the techniques, procedures and functions developed during the project lifetime. The objective would be to test the developments coming from other WPs over real environments, with real users, facing all the constraints and limitations that a complex society can pose in these kinds of trials.

The architecture (WP1) and the trust and communication framework (WP2/3) are generic enough to be applied to a large number of use cases. Amongst these, two illustrative examples (supportive, lean and safer communities) will be selected, so as to assess the feasibility of the architecture and mechanisms developed in the project and to bring the citizens services of high societal value.

In order to reach the aforementioned goals, this WP will particularly tackle the following objectives.

- O5.1: To specify two pilot trials by further elaborating selected use cases proposed in WP1.
- O5.2: To analyse the operation and performance of the implemented innovations developed in other technical work packages and providing feedback for the optimisation of the initial designs
- O5.3: To pilot two services in the cities in order to assess the appropriate fulfilment of the initial objectives of SOCIOTAL by larger-scale evaluation findings and usability feedback from both end user and developer communities.

1.2.1 Task 5.1 Trial and pilot specifications

Based on the architecture provided by WP1 and the various techniques, procedures, and protocols provided by the rest of the WPs, this task will specify the trials to be used during the experimental evaluation. The specific needs from the end-users will be also considered, and detailed and systematic evaluation procedures will be designed, so as to be able to gather feedback from the trial end-users. The design will also take into consideration the capabilities of the platforms over which the trials will be conducted (for instance, the SmartSantander testbed).

1.3 Purpose of the deliverable (DNET)

This report will describe the scenarios selected for the field trials and pilot deployment, together with the evaluation methodology, including relevant KPIs; those will be based on the evolved use cases provided by WP1.

Section 2 - Field trials (DNET)

In this section selected field trials will be explained in details. Firstly trial evaluation process is described. Different target groups are specified (end users, SW and HW DIY (do it yourself) and Service developers) and the ways of interaction with these groups, and the expectations in terms of evaluation. The enablers to be developed during the project life will be evaluated in different phases and within each step a target group (or several) will be approached. For each trial are presented the scenario and the use cases extracted from it in addition to the key performance indicators. The following enablers will be tested:

- Registration enabler (Registering users/devices)
- Discovering people, devices and resources around the user, data uploa/download
- Community creation/update
- Evaluating mood of the city
- Elevator supervisor
- F2F enabler
- Privacy-Preserving reputation and discovery
- User trust tool evaluation
- IdM and Access Control mechanisms between Bubbles evaluation
- Secure Group sharing mechanisms evaluation
- Location-aware Access Control for indoor environment evaluation

2.1 Trials Evaluation process (UC)

This subsection describes the general evaluation process for the trials to be developed within SocIoTal project. The main objective of these processes is to gather, from every trial's set of final users, the results of testing each tool/s and/or enabler/s involved, using the mechanisms defined through this text. On the other hand, besides the technical part or the user interfaces, the process will also evaluate the incentives to promote the users enrolment, in order to be improved in regards to the final pilots. These evaluations will detect, in addition, bugs and malfunctions as well as collect suggestions that lift the user's experience.

2.1.1 Trial description

Throughout this report, a complete description of every envisioned field trial, including the involved tools and enablers and the evaluation pursued objectives, will be provided. The mentioned descriptions will present a main scenario that tells the general environment where the trial is planned to be played, including a set of related use cases that focus on testing different features of the general trial. These trial descriptions are oriented to accomplish the objectives of the task 5.1, this is, to show the trials in the context of SocIoTal project, relating them to the progress and technical innovations achieved in the rest of WP involved. A shorter and user's centric description of every trial will be distributed among the trial's user group, including:

- Short and non-technical description of the overall trial, presenting the different tests to be performed and the main objectives of the evaluation.
- A simple guide or tutorial, oriented to the trial's user, showing the management of the tools and enablers
- Instructions to perform the tests and provide the feedback

2.1.2 Selection of user groups

Parallel to the trial description, the different target groups, according to every trial, will be specified. Here is also included the ways of interaction with these groups and the expectations in terms of evaluation.

As a result of WP6 efforts the different target groups will be attracted from local events, co-creation workshops and Meetups throughout the project life. Through this events and activities the project interacts with all participants and gathers feedback regarding the potential usage of the project outputs as well as new requirements, potential additional functionalities, features that the SocIoTal solution should provide and also a rich evaluation in the different evaluation phases. The following target groups are considered at the moment:

- End users: citizens not directly involved in technology, i.e. people who has electronic devices such as smart phones, tablets, computers, etc. but are not technical experts. These people will be approached through Meetups and other workshops that aim to explain to the user the use cases and allow them to participate in its improvement.
- SW and HW DIY: (Software and Hardware do it yourself) citizens with a higher level than "user-level" knowledge but without being experts. These users are curious to create their "homemade" devices and to investigate how to create little things with cheap components.
- Service developers (SW and HW): this group involved in the creation of high value services and application for the society will provide more specific and technical feedback which will help the project to capture new requirements, new possible features, technical bugs or malfunctions.

The enablers and tools to be developed during the project life will be evaluated in different phases and within each step a target group (or several) will be approached. Firstly, the first version of the enabler will be evaluated internally within the project partners. This phase has the purpose of fixing first bugs and malfunctions. A following version of the enabler will be evaluated by end users, citizens and developers selected from workshops, and people amateur in SW and HW interested in the project. In order to obtain a complete evaluation that aims to have a final and stable version of the tool, a questionnaire will be distributed to the different target groups at the end of the experiment. Also, an email will be provided in order to report bugs, malfunctions, suggestions, etc.

2.1.3 Key Performance Indicators (KPI) definition

Defining a Key Performance Indicator within the SocIoTal context as a measurable value that demonstrates how effectively a trial performance is achieving its key objectives, the trial evaluation process will use KPIs to evaluate the success at reaching tools, enablers and mechanisms targets. This way, KPIs help SocIoTal understand how well it is performing in relation to its strategic goals and objectives. In the broadest sense, a set of KPIs can tell whether the field trial and the SocIoTal elements involved is on track or not.

Some of the KPIs are common (the same) for a few scenarios and are numbered with the same KPI ID. For the sake of completeness, i.e. to allow reader to follow KPIs specific for observed scenario, full descriptions of these KPIs are repeated for every single scenario where they are used but with unique ID (for example KPI 001 Number of Evaluators). Some KPIs have the same name (like KPIs 002 and 008: Tools Usability) and perform the same measures, but evaluate different tests (for example KPI 002 performs test: Create a new SocIoTal user/identity, while KPI 008 performs test: Using the community Management Tool to create/update/modify/delete community

Every field trial will define its own set of KPIs, reducing here the complexity of the evaluation process to the track of a small number of parameters, in order to make performance more understandable and digestible for the evaluators.

The field trials specified along this document will include, as a main subsection, the set of KPIs identified within its context and considered to help its performance evaluation. Every presented KPI will report:

- Definition, as the selected KPI literal description
- Unit (of measurement), representing what kind of measurement it will provide
- Criteria, as the way the KPI is going to be measured or considered
- Relevance, reflecting the importance of the KPI and/or the impact it has related to the performance of one or several of the tools, enablers or methods evaluated

2.1.4 Trial Planning

This part of the trials specifications presents an initial overall view of the whole testing process, showing the different stages times, what and when enablers and prototypes are deployed, the users involved, the evaluation times and the feedback collected impact over the elements tested.

Although each reported trial will present differences on its initial planning depending on the enablers to be tested, the users to be involved or the deployment capabilities required, the main stages that compose most of them are:

1. Prototypes (enablers & tools) involved development: details which SocIoTal enablers and/or modules will be prototyped and tested in the trial. It provides also the time needed to develop these initial prototypes and the functionalities offered.

2. Lab Testing: during this stage, the prototypes (beta versions) will be subjected to several lab tests, before the first alpha version can be deployed for a real scenario testing.

3. Users Enrolment & Trial deployment: once the prototypes are ready, they will be deployed and linked with other enablers and/or functional modules needed to build the test environment. In parallel, the different selected set of trial users and developers will be engaged and introduced to the trials enablers, functionalities and objectives.

4. Trial evaluation & Feedback Collection: with the trial environment available and the selected users trained, it's time to perform the evaluation process indeed. The different ways these evaluation processes will be performed in each trial will provide valuable feedback from users and developers that need to be collected to be later used in the last stage.

5. Corrective & Improvements actions: this gathered feedback from final users will report, apart from their user experience, bugs detected in the alpha version as well as suggested improvements that could be integrated into new upgraded versions of the SocIoTal enablers and tools, oriented to the service pilots.

This set of stages describing the trials evaluation performance will be distributed mainly along the second year of the SocIoTal project, starting officially on M16 and ending on M27, led by Task 5.2 of the project.

2.2 SocIoTal Context Management Tools: register, discover and context data management trial

This trial will carry out a set of tests over the SocIoTal Context Management tools that allow the final user to create a profile, register a device, upload context data to share and discover other users/resources from where to obtain information. The trial will be composed of several scenarios that present the different use cases for each test. In turns, each test will focus on a baseline functionality that should be provided by SocIoTal, in order to build on top, later on, the whole service pilots with advanced SocIoTal features.

2.2.1 Scenario 1-1: Registration of User and Devices/Resources

First step, within SocIoTal, will be to create and register an "identity", associated to a user, in order to be identified and authenticated before executing any other SocIoTal activity. Next step, if the user wants to upload and share information, would be to register the resource (device, smart object, information source, etc.) that will generate the context data. This scenario presents the users' need to get registered in SocIoTal's platform before being able to register their resources to report and share information, as well as to join or to create communities and/or bubbles.

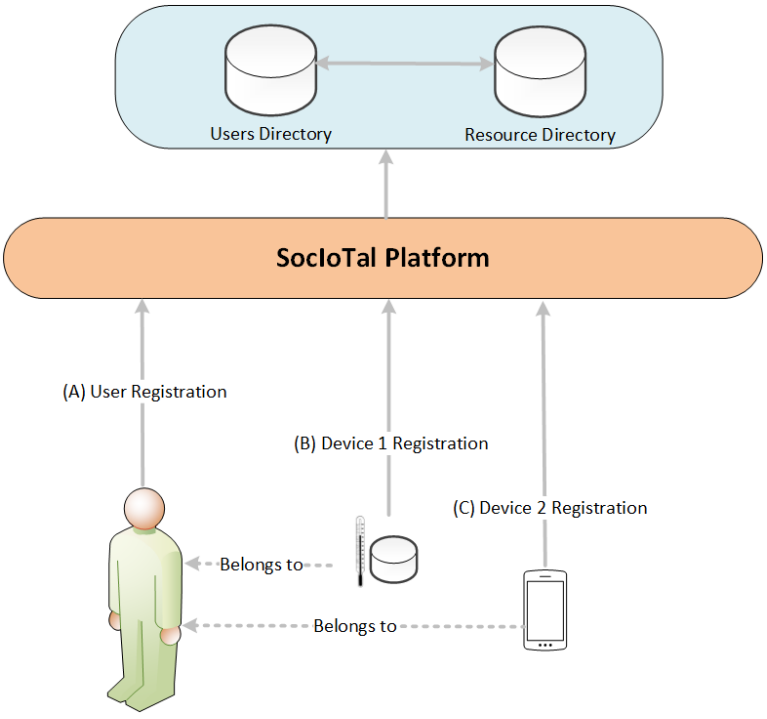

Figure 1. Registering with SocIoTal

The process is represented in Figure 1:

1. Access to the registration tool (via a user interface: web, mobile application, etc.)
    - Identification & authentication process if the user has been previously registered
2. Fill the information required to register users/devices/resources

- Profile info (attributes/values) to define the user (A)
- Context Data info (entity attributes/values) to define devices/resources (B)

3. Push the information to the SocIoTal platform (user/resource directory)
4. User reception of an acknowledge message indicating the proper execution of the registration process

Additionally, and according to the final SocIoTal Security framework implementation, the user will receive (when registering) the corresponding security token to be identified and authenticated in their further requests (e.g. to register a new resource or upload new context information).

The first scenario's trial will allow the evaluation of the SocIoTal Registration tool that provides a set of methods to register users, devices and resources in the simplest way possible. These methods, that conform an API (Application Programming Interface), will be used directly, through a specially designed user interface (SocIoTal's User Environment), by the final user to get registered together with their resources, or integrated in a user application that captures the needed data and performs the corresponding registering process. The Registration tool will interact later with the corresponding platform resource directory to properly register devices and with the user's directory, assisted by the SocIoTal's Security framework, to check the user credentials and/or register a new user. Figure 2 presents the initial scheme for the Registration tool, including its envisioned functionalities and blocks. This tool will be further described and developed in WP3 deliverables (D3.2 [1] and D3.3 [2]).

Figure 2.SocIoTal's registration tool initial diagram

2.2.1.1 Use case 1-1.1: registering users

The first step to make use of the SocIoTal platform is the registration. The tool will allow a potential user to fill the required data through a friendly interface. After that, the information provided will be formatted following the *User Data Model* and sent to the Identity Management module, i.e. the User's

Directory. Once the user's registering process has been successfully completed, the user will get the security credentials/token (as will be specified by the SocIoTal Security Framework) to allow their devices registration, modification and interaction with SocIoTal's platform, as well as data uploading/downloading.

2.2.1.2 Use case 1-1.2: registering a device

Once the user has completed their registration, they will be empowered, by means of the resulting token, to register her devices and the resources she can provide. In a similar way, the user will complete the information about their devices and resources (entity and attributes). The user's credentials/token will be checked and then, the resource registration data will be pushed to the Resource Directory module.

2.2.2 Scenario 1-2: People and Resources discovery

One of the key points of the SocIoTal project is the ability to discover people, devices and resources "contextually close" to the user. In this sense, they will be able to trigger a discovery process filtering by different properties such as distance, entities, attributes, etc.

The current scenario provides the environment to test the *SocIoTal Discovery Tool*, based on context information already available in the centralized platform. It will provide the user with an API to perform searches and discovering processes, using attributes and data from the users/resources context. The Discovery tool shown in Figure 3 further presented and developed within WP3, will provide the user with such functionalities.

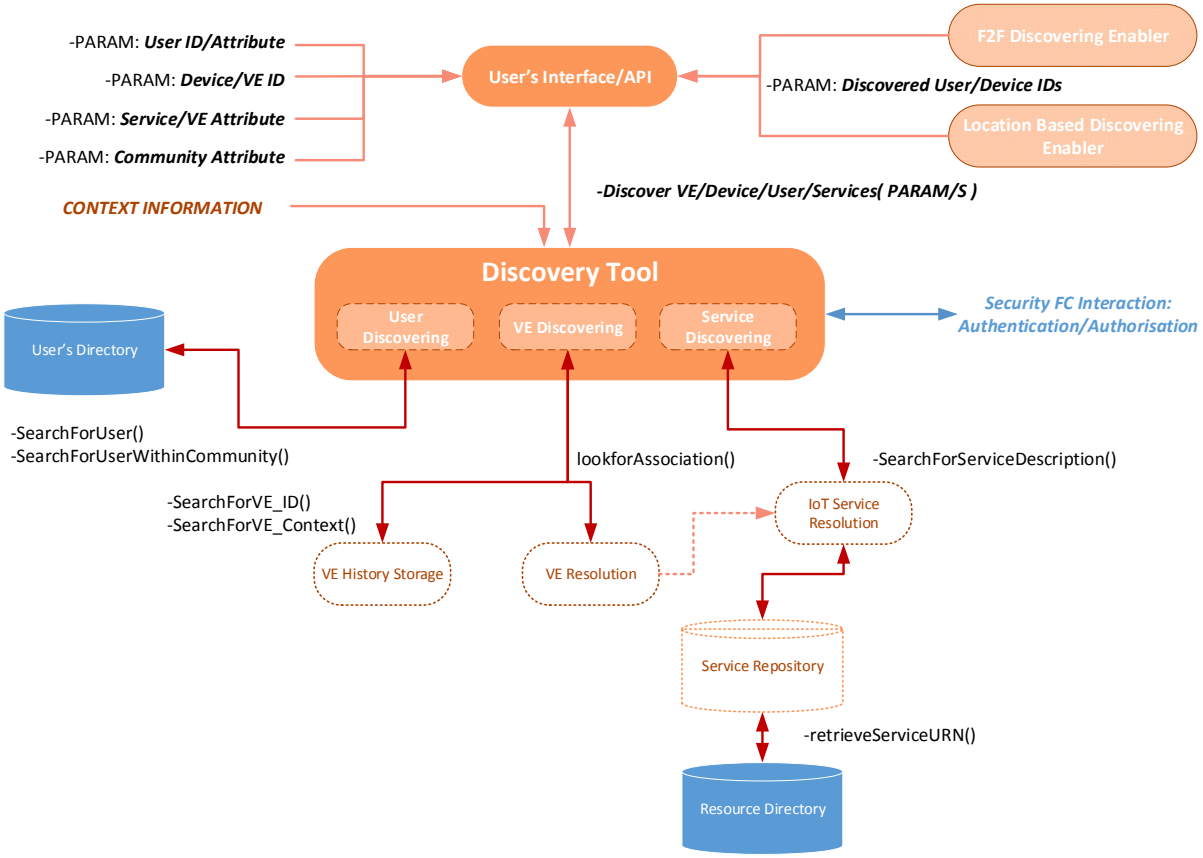

Figure 3. Discovery tool initial diagram

According to this, the scenario description is as follows: a citizen has an appointment with some friends. As the pub is crowded, he decides to trigger the discovery process through the SocIoTal tool in his mobile and filter by people from his "friends' community" 20 meters around to discover if some of them are in the pub. The application will discover all their friends that have allowed the application to gather their position in order to be discovered by people from their communities. As three friends are already there, he received the response with the position of those three members in the pub.

Once they have meet all, they start planning a route for the next day in a village not far from the city. To be sure about the weather conditions in the village they launch the discovery process for temperature/humidity observation in that area.

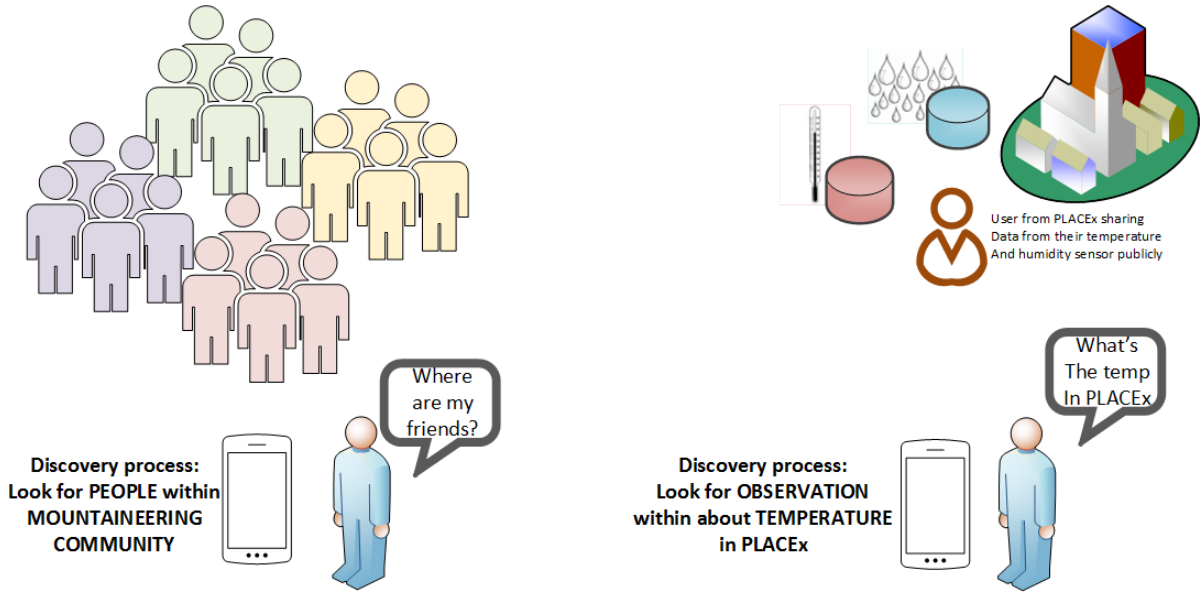

Figure 4. Discovering examples

From the above there can be extracted different specific features:

- Access the discovery tool (via a user interface: webpage, mobile application, etc.)
- Launch discovery process
- Complete data required and select filters to form the request
- Push the request to the platform
- Receive the response from the platform

2.2.2.1 Use case 1-2.1: Discovering people

To improve the sharing information process between users, different types of discovery are implemented within SocIoTal. In one hand, through this tool users will be able to discover other people using different filters such as geolocation, community to which they belong, etc.

2.2.2.2 Use case 1-2.2: Discovering information sources

On the other hand, users could be interested in resources or information instead of other people. In this case they will be able also to discover the resources available to them filtering by different context attributes (geolocation, entities, attributes, etc.).

2.2.3 Scenario 1-3: Data upload/download

This scenario complements the registering and discovering ones with the tool (API) supporting the upload of new context info from a registered resource owned by an identified user and getting context from a discovered resource (sharing info) to an authenticated user or device. This part of the trial is focused on using the API to upload information (measurements, observations, events, context data, etc.) and download (access) required data from other devices/users. These API's tests will be driven through the trial user that will be previously identified and authenticated using their identity and credentials for then, trigger the upload actions and/or the info requests. However these tests are totally analogous to a smart objects scenario, where "autonomous devices", using their own identity or the one associated to its owner to get access to the platform.

2.2.3.1 Use case 1-3.1: upload data

Once the user has been properly registered and their identity has been created, after the corresponding authentication process, they will call the function to upload data from their resources. During the trial (Figure 5), the user will be requested to report an event by taking a photo from his/her device and adding an explanatory text. By means of a user-friendly user interface this information will be merged and sent to the platform through the SocIoTal API for uploading data.

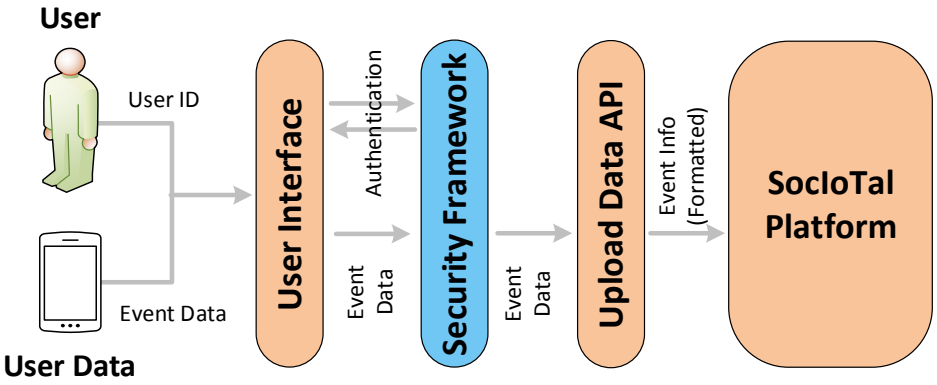

Figure 5. Uploading data test

2.2.3.2 Use case 1-3.2: get information

On the other side, once the user has granted (according their credential) access to SocIoTal platform (or the corresponding SocIoTal app), they can request information they are allowed to get. During this trial execution, the user will be requested to "discover" all events reported around a given location and/or within a time interval and select some of them to get the associated info (text and photos). The schema of this test is shown in Figure 6

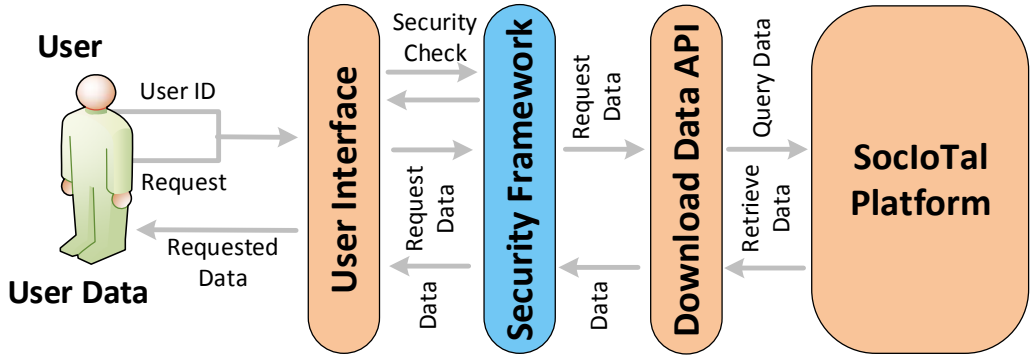

Figure 6. Downloading data test

2.2.4 SocIoTal Context Management Tools Key Performance Indicators (KPI)

According to the trials evaluation process, this section presents the selection of Key Performance Indicators that will be used in the assessment of the SocIoTal Context Management tools described above. These KPIs cover different aspects of the tests to be performed trying to include both, subjective parameters, like the user experience using the provided tools, and objective ones such as performance times or failure rates. Following tables present an identifier for the KPI, its name, a definition, the unit of measurement, the criteria followed for the evaluation and the relevance of the KPI compared to the other measurements in the list.

For all tools, the selected KPIs are:

KPI Id:	001	KPI title:	Number of evaluators
Definition:	Number of people from the target groups that will evaluate the corresponding tool/API.		
Unit:	Number of people		
Criteria:	The greater the number of people who evaluate the trial, greater the success of the KPI.		
Relevance:	Medium relevance. It is not considered as high relevance because even if there are not many people involved in the evaluation it can be successful if the most failures and interesting improvements are discovered.		

KPI Id:	002	KPI title:	Tools Usability
Definition:	Usability measures the grade of simplicity, adaptability and functionality perceived by users when they perform the corresponding tests through the provided tools: - Create a new SocIoTal user/identity - Register a device/resource - Upload info from the resource - Discover available info - Perform a request and get the requested info This indicator will be extracted from questionnaires distributed among the participants, according the valuation scales provided.		
Unit:	Scale from 1 to 10		
Criteria:	Low levels of the scale represent low levels of usability while high levels represent a high level of satisfaction on the experience in the use of the tool.		

Relevance:	High relevance. The usability is one of the strong points of the SocIoTal tools.

KPI Id:	003	KPI title:	General Tool crashes ratio
Definition:	Percentage of tool crashes during its usage, due to APIs malfunction coming from issues out of SocIoTal development (selected platform crashes, communication links failures, etc.).		
Unit:	Percentage		
Criteria:	A high percentage of application crashes results in a low performance. Failure ratios over 10% may result in selected platform reconsideration.		
Relevance:	High relevance. The number of application crashes has to be as lower as possible in order to improve the degree of comfort in the use of the tool.		

KPI Id:	004	KPI title:	Process performance time
Definition:	Time the user takes to execute (prepare and send the request and receive the response) the corresponding procedure: - Create a new SocIoTal user/identity - Register a device/resource - Upload info from the resource - Discover available info - Perform a request and get the requested info It will be measured from the point of view of the final user, involving all the times from the user starting to introduce the corresponding process needed info through its interface till the response of the called process is shown to the requestor.		
Unit:	Seconds		
Criteria:	Capture the time the user takes to perform a whole procedure. Repeat the process with different kind of users in order to get enough data to perform statistical analysis.		
Relevance:	Medium relevance. The different statistical parameters extracted from the measurement of this KPI (average time, variance, etc.) will show how the tool performance is among different set of users (non-geek users, developers, etc.)		

KPI Id:	005	KPI title:	API Usability
Definition:	API usability measures the grade of simplicity, adaptability and functionality perceived by users (mainly developer – geek users) when they perform the corresponding tests through the provided APIs: - user registration - resource registration - discovering request - data upload - data request This indicator will be extracted from questionnaires distributed among the participants, according the valuation scales provided.		
Unit:	Scale from 1 to 10		
Criteria:	Low levels of the scale represent low levels of usability while high levels represent a		

	high level of satisfaction on the experience in the use of the tool.
Relevance:	High relevance. The usability is one of the strong points of the SocIoTal APIs.

KPI Id:	006	KPI title:	Failed process execution ratio
Definition:	Percentage of errors occurred during the execution of the analysed process: - user registration - resource registration - discovering request - data upload - data request		
Unit:	Percentage		
Criteria:	Failures reported due to developed API/Process will be here considered. A high percentage will represent a high level of failures in the analysed process. Percentage over 10% will require immediate corrective actions. Due to the initial complexity of discovering processes, here a percentage over 20% will be considered		
Relevance:	High relevance. The number of internal process crashes must be as low as possible.		

KPI Id:	007	KPI title:	Procedure (API) response time
Definition:	Related to the time the procedure API takes to retrieve Ok once it's been called. Measures ONLY the response time of the developed procedure, called through its corresponding API and deployed on the trial platform. Processes to be analysed will be: - user registration - resource registration - discovering request - data upload - data request		
Unit:	Milliseconds.		
Criteria:	Measures the response time due to procedure algorithms, platform iterations and communication technologies used. These times will be collected through the logs of the SocIoTal server.		
Relevance:	High relevance. These procedure response times should drive the whole corresponding process performance. The lower performance time, the faster the retrieving is and the better user experience should be.		

2.2.5 SocIoTal Context Management Tools initial trial planning

According to the general trial evaluation process, the different stages, actors and elements involved in the above mentioned functional tools test will be:

1. Prototypes (enablers & tools) involved development: the ere described scenarios will test the initial beta versions of the:
    - Registration tool, to create new users/identities and add resources to the platform

- Discovering tool, that provide the functionalities to find users, resources and set of data
- Upload Data / Retrieve (download) Data APIs to perform the data and context sharing/access features

As the different diagrams of the tools provided show, these tests will also involve the SocIoTal Context Manager and the selected platform users and resource directories. It will also include, as far as possible and as appropriate, the integration with the SocIoTal Security framework defined within WP2/3 and the Users Environment provided by WP4.

The initially planned time to get the first beta versions to be tested in lab is 5 months within Task 5.2, including also the integrations needed, although some initial works have already started before.

2. Lab Testing: starting on M17, different tests related to API implementation, FI-WARE integration and interoperability within SocIoTal environment will be performed in the UC labs. For these purposes, an initial SocIoTal platform mock-up, including some of the SocIoTal elements, such the SocIoTal Context Manager, will be developed to test every tool functionality before been released.

3. Users Enrolment & Trial deployment: when first beta versions of the Functional tools have been properly tested in UC premises, a first instance of the SocIoTal platform will be deployed, including all functional blocks and services needed to perform the tools trial. In parallel, through the IoT Meetups and the different workshops planned during the first half of the second year of SocIoTal, a set of trial users will be selected to participate in the different tests programmed:
   - Final users (standard user profile). Around 30 envisioned participants will test, through the users interface provided, the functionalities and performance of the SocIoTal functional tools.
   - Developer Users (geek users/developers profile). Around 20 envisioned participants will directly work with the tool APIs provided, testing the feasibility of these APIs to be integrated within other environments (their own user interfaces).

4. Trial evaluation & Feedback Collection: to be started on M24 and, during two months, the selected set of users will be provided with the user interfaces and the APIs access needed to perform the different tests that compose this trial. These tests performance will be specified during the lab validation of the prototypes, according the way these developments are built and focused on the KPIs to be collected. A description of the trial, the steps and all info needed to play them will be provided to participants before the trial starts.

5. Corrective & Improvement actions: as soon as the trial starts, the bugs reporting will be also opened.

According to defined KPIs for this trial, bugs and malfunctions that directly affect to execution and performance times will be expected to be the most relevant ones and will be considered as high priority.

The feedback collection (to get suggestions, improvements and so on) is expected to start providing valuable information during the second half of the stage 4. This time, the evaluation of these initial set of corrections, suggestions and improvements will be evaluated by UC developers in order to implement as far as possible those relevant ones, to be available for the pilots.

A diagram of the SocIoTal Functional Tools initial planning for the trial is shown in Figure 18

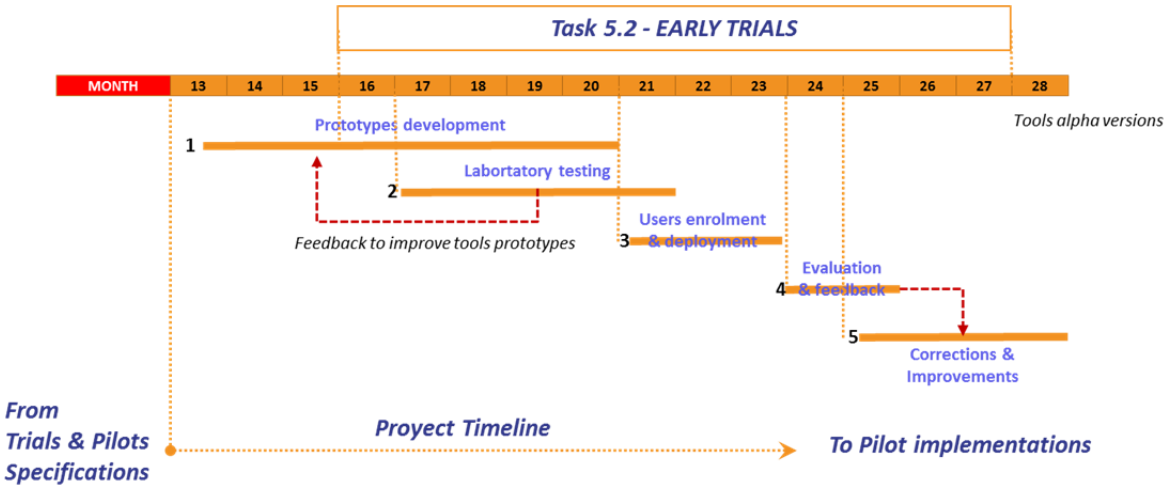

Figure 7. Functional tools trial initial planning

2.3 Community Management Tool

One of the most important barriers in the Internet of Things user's acceptance is the data privacy. When users want to share information about them, their devices, etc. they do only share it with people they trust and being totally sure that no one else will access that information and that there is not information leakage.

This tool gives the user the control of data sharing, allowing it only with people properly identified and authenticated. In order to do that, the tool enables the creation of groups and its management through different functionalities such as owner assignation, specific community storage creation, add/remove user/resources/storage, define and modify security policies, etc. A first approach to this tool, which will be developed within WP2 and WP3 is shown in Figure 8.

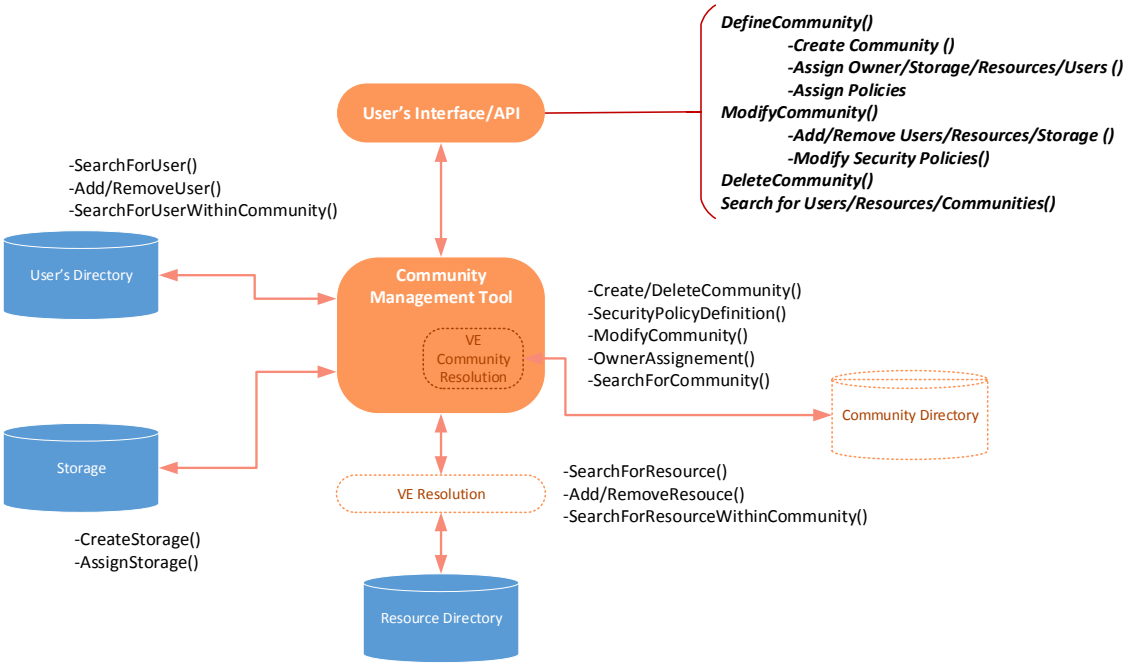

Figure 8.SocIoTal's Community Management tool initial diagram

2.3.1 Scenario 2-1: Creating a Community to share information

A group of weather enthusiasts created an association to share their knowledge about weather. They realized that it was difficult to share the information through the internet from the devices they had built or bought without sharing that information with other people out of the association easily. For that reason they decide to register themselves and their devices within the SocIoTal platform, and entrust the creation of a Community to the president of the association. To create the Community, the president fills the data needed such as the owner of the community, the storage where the info will be kept, the users that will conform the community, some resources and policies to access the data, etc. Once the community has been created and the users has been included as members they can start to add devices and resources to the Community. Now, they can access to the resources offered by the other members safely without information leakage.

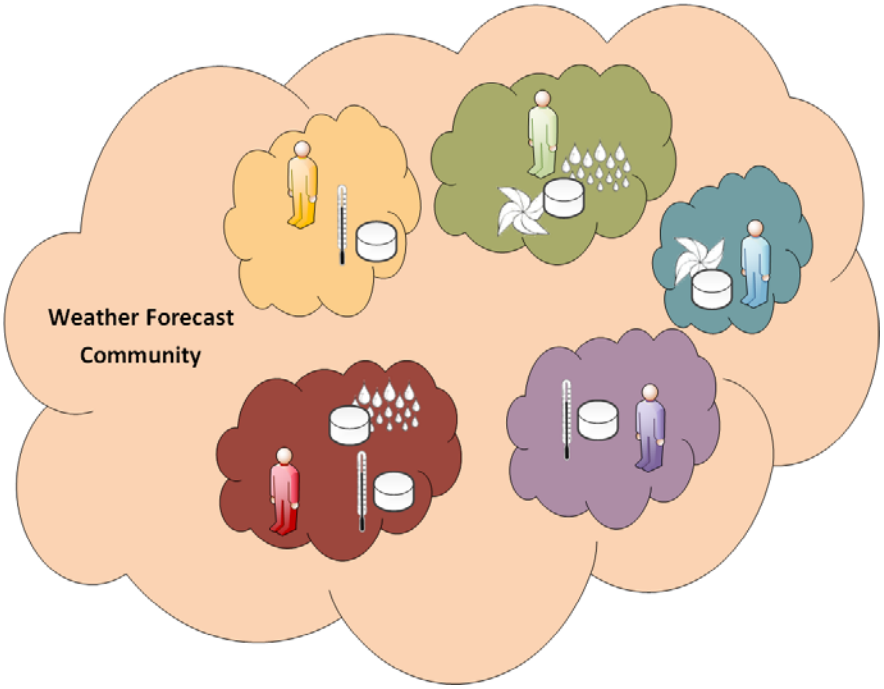

Figure 9. Communities example

From the scenario described in Figure 9, there can be extracted the following use cases:

- Access the tool through the user interface (webpage, mobile application, etc.).
- Community Creation providing the minimum required data:
  - Administrators of the community
  - Storage
  - Access policies
  - Members
  - Resources to add, etc.
- Update community information to the platform:
  - Add/modify/delete users
  - Add/modify/delete resources
  - Change administrators
  - Change storage capacity
  - Delete community, etc.

2.3.1.1 Use case UC2-1.1. Community Creation

In order to share information within a group among people without information leakage, users will be able to create a community through the SocIoTal Community Management tool. Thus, they will share information (sensor data, links to stored information, photographs, etc.) among the community members within a safe environment.

2.3.1.2 Use case UC2-1.2. Community Update

Once the community has been created, members will be able to modify different aspects of the community, each depending on the permissions they have within the community. Members with higher permissions (such as the creator/administrator) will be able to add new members to the

community, remove them, change the storage capacity or delete the community among others. However, users with less permissions will be able for example to add new resources from their devices or remove themselves from the community.

2.3.2 Community Creation tool Key Performance Indicators (KPI)

Tables below present the selected Key Performance Indicators for the Community Creation Enabler trial. These KPIs will cover different aspects such as the number of users to evaluate the trial, usability for the evaluators or technical KPIs as enabler malfunctions among others. These tables describe an identifier for the KPI, its name, a definition, the unit of measurement, the criteria followed for the evaluation, and the relevance of the KPI compared to the other measurements in the list.

KPI Id:	008	title:	Usability
Definition:	Usability measures the grade of simplicity, adaptability and functionality perceived by users when they perform the corresponding tests: - Using the Community Management tool to create/update/modify/delete a community through the User Environment (from WP4) (normal profile users) - Using the Community Management tool API to create/update/modify/delete a community (geek users/developers profile) This indicator will be extracted from questionnaires distributed among the participants, according the valuation scales provided.		
Unit:	Scale from 1 to 10		
Criteria:	Low levels of the scale represent low levels of usability while high levels represent a high level of satisfaction on the experience in the use of the tool.		
Relevance:	High relevance. The usability is one of the strong points of the SocIoTal tools.		

KPI Id:	009	title:	CM Tool crashes ratio
Definition:	Percentage of tool crashes during its usage. This KPI will distinguish among: - Failures due to APIs malfunction coming from issues out of SocIoTal development (selected platform crashes, communication links failures, etc.). - Failures due to internal APIs algorithms or procedures that directly may require corrective actions. Also, this KPI will cover: - Community Creation failures - Community management operations (update, modify, delete) The reported crashes and the logs of the APIs will be used to capture this KPI		
Unit:	Percentage		
Criteria:	A high percentage of tool crashes results in a low performance. - Failure ratios over 10% attributed to external issues may result in selected platform reconsideration.		

	- Failure ratios over 15% attributed to internal APIs issues will require immediate corrective actions.
Relevance:	High relevance. The number of tool crashes (regardless of the incidence origin) has to be as lower as possible in order to improve the degree of comfort in the use of the tool.

KPI Id:	010	title:	Process performance time (User Interface)
Definition:	Time the user takes to execute (prepare and send the request and receive the response) the corresponding procedure: - Using the Community Management tool to create/update/modify/delete a community through the User Environment (from WP4) (normal profile users)		
Unit:	Seconds		
Criteria:	Capture the time the user takes to perform a whole procedure. Repeat the process with different kind of users in order to get enough data to perform statistical analysis.		
Relevance:	Medium relevance. The different statistical parameters extracted from the measurement of this KPI (average time, variance, etc.) will show how the tool performance is among different set of users (non-geek users, developers, etc.)		

KPI Id:	011	title:	Process performance time (API response time)
Definition:	Time the user takes to execute (prepare and send the request and receive the response) the corresponding procedure: Using the Community Management tool API to create/update/modify/delete a community (geek users/developers profile)		
Unit:	Seconds		
Criteria:	Measures the response time due to procedure algorithms, platform iterations and communication technologies used. These times will be collected through the logs of the SocIoTal server.		
Relevance:	High relevance. These procedure response times should drive the whole CM management processes (including the request creation, performance and data retrieving to the user interface). The lower performance time, the faster the response is and the better user experience should be.		

2.3.3 Community Management tool initial trial planning

Community Management is one of the key factors of SocIoTal goals, so it is envisioned to interact and integrate with most of the SocIoTal enablers and tools. This characteristic conditions its trial planning to the availability of initial prototypes or, at least, initial descriptions, of several SocIoTal elements. Having this in mind, the initial trial planning according the above mentioned general stages is described in this subsection:

1. Community Management tool Prototype development: the presented scenario 2-1 will test the initial beta version of the Community Management tool. This will also test the integrations, as far as possible and as appropriate with:
    - Platform Users' Directory, to check users' identities/profiles and add users to the community.

- Platform Resource Directory, to also check and add resources to the created community.
- Platform Storage capabilities, to create and manage specific storage space for the information uploaded and shared within community users (when needed).
- SocIoTal Security Framework (from WP2/3), in order to perform the security actions needed to identify and authenticate the coming requests (data, membership, modifications, etc.). Interactions with the Identity Manager (IdM), Group Manager (GM) and Access Control (AC) element will be required.
- SocIoTal User Environment (from WP4), to provide an interface for the final user to access the Community Management tool API.
- SocIoTal Context Management Tools, with the needed APIs to upload, discover and access shared info within the created communities.

The development of the CM tool will need from the Security Framework to define users' profile and identification/authentication mechanisms within SocIoTal. According to this, development will start during M16, when these first security issues were available. Mechanisms also to define and create communities and bubbles will be needed and tested here.

2. Lab Testing: starting on M18, different tests related to different elements of the CM (API REST, development framework, functionalities implementation and performance…), FI-WARE integration and interoperability within SocIoTal environment will be performed in the UC labs. For these purposes, an initial SocIoTal platform mock-up, including some of the SocIoTal elements, such the SocIoTal Context Manager, the IdM, the Access Control or the Group Manager will be developed to test every tool functionality before been released.
3. Users Enrolment & Trial deployment: when first beta version of the Community Management tool have been properly tested in UC premises, a first instance of the SocIoTal platform will be deployed, including all functional blocks and services needed to perform the tools trial. In parallel, through the IoT Meetups and the different workshops planned during the first half of the second year of SocIoTal, a set of trial users will be selected to participate in the different tests programmed:
    - Final users (standard user profile). Around 30 envisioned participants will test, through the users interface provided, the functionalities to create a community and manage it, and also evaluate the CM performance.
    - Developer Users (geek users/developers profile). Around 20 envisioned participants will directly work with the tool API provided, testing the feasibility of this APIs to be integrated within other environments (their own user interfaces).
4. Trial evaluation & Feedback Collection: to be started on M24, together with the Context Management Tools and, during two months, the selected set of users will be provided with

the user interfaces and the APIs access needed to perform the different tests that compose this trial. These tests performance will be specified during the lab validation of the prototypes, according the way these developments are built and focused on the KPIs to be collected. A description of the trial, the steps and all info needed to play them will be provided to participants before the trial starts.

5. Corrective & Improvement actions: based on the KPIs provided for the Community Management Tool, the different performance times are expected to be (as with the Context Management Tools) the higher priority bugs and corrective actions source. All the issues that have to do with this will be fixed before alpha version release.

   The user feedback collection (to get suggestions, comments and so on) will be evaluated by UC developers focused on highlight the user experience by considering all new features (and the execution of the existing ones) suitable to improve the overall performance of the Community Management.

A diagram of the Community Management tool initial planning for the trial is shown in Figure 24.

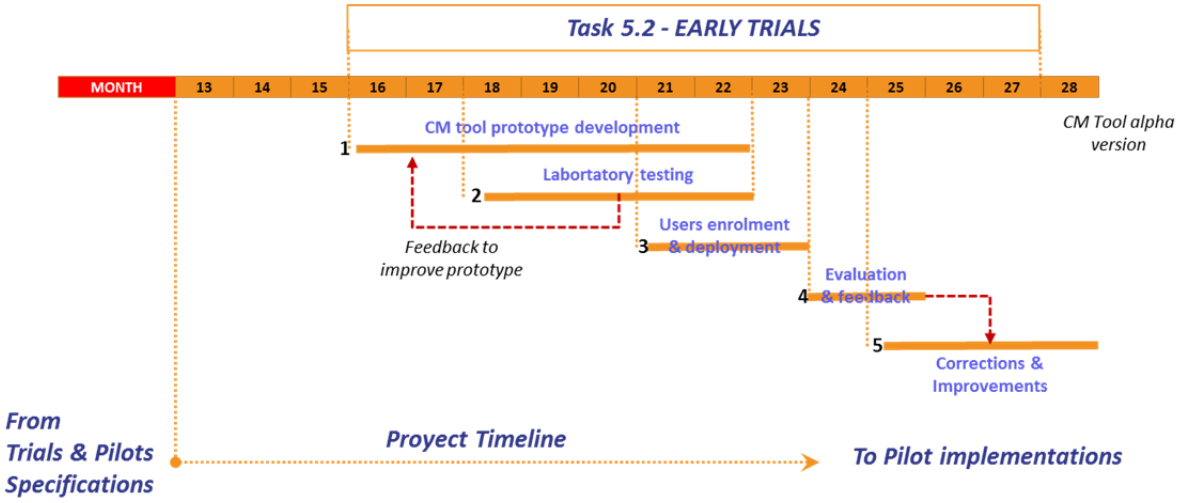

Figure 10. Community Management tool trial initial planning

2.4 Evaluating Mood of the city (DNET)

There are previous approaches for assessment of peoples' mood [3] and happiness [4], [5]. We have tried to provide a joint metric that will help citizens to measure mood in the city by introducing contextually different parameters [6] to previous approaches.

This trial will allow the evaluation of the mood of the city enabler that offers to the users a method to evaluate their mood based on data entered (i.e. current image of themselves and answers to the specific question) as well as based on current environmental data collected from ekoBUs700++ device [7](Figure 11).

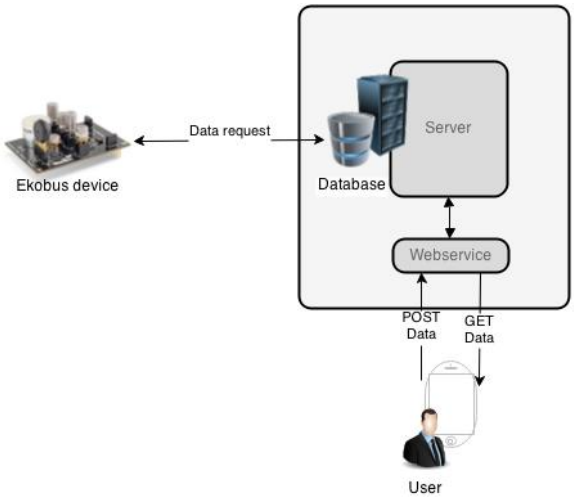

Figure 11. Sending and getting data from user and sensors

2.4.1 Scenario 3-1: Mood of the city

A group of friend was excited when one of them was discovered application that can identify their mood based on their facial expression. Each one of them was playing with camera that can detect mood, and then after populating questionnaire, their final mood was displayed on screen together with total mood of the city index of all citizens that posted their data.

2.4.2 Use case UC 3-1.1: Collecting environmental data

Environmental data, i.e. humidity and temperature are summoned from ekoBUS700++ device, a sensor board attached to a rooftop of a public transportation vehicle in Novi Sad. These data is gathered each several hours and saved in the local database. User can see these data via Android mobile application.

2.4.3 Use case UC 3-1.2: Collecting user's mood data

This main functionality of this use case is mood detection from the users' facial expression as well as collection of the users' happiness index by using happiness index questionnaire. User by using mobile application's camera detects his/her mood and then populates questionnaire, with a set of questions commonly used in scientific community for evaluating peoples' happiness.

2.4.4 Use case UC 3-1.3: Computing mood of the city index

This use case is focusing on several functionalities offered to the user in order to compute the final mood which is going to be presented to the user. Data gathered from the UC's for all users is then combined and used to compute mood of the city index. Inputs are scaled to a predefined maximum impact factor that each parameter has and then final value is given to the user as overall summation ratio of all inputs.

2.4.5 List of Key Performance Indicators (KPI)

This section presents a set of tables which shows the Key Performance Indicators selected for the trial of the mood of the city enabler. These KPIs will cover different aspects such as the number of users to evaluate the trial, the look and feel perceived by the user their perceptions or technical KPIs as enabler malfunctions among others. These tables describe an identifier for the KPI, its name, a definition, the unit of measure, the criteria followed for the evaluation, and the relevance of the KPI compared to the other measurements in the list.

KPI Id:	001	KPI title:	Number of evaluators
Definition:	Number of people from the target groups that will evaluate the Mood of the city enabler.		
Unit:	Number of people		
Criteria:	The greater the number of people who evaluate the trial, greater the success of the KPI. Depending on the evaluation phase the correspondent target group will be selected.		
Relevance:	Medium relevance. It is not considered as high relevance because even if there are not many people involved in the evaluation it can be successful if the most failures and interesting improvements are discovered.		

KPI Id:	012	KPI title:	Usability
Definition:	Usability measures the grade of simplicity perceived by the users when they use Mood of the city application.		
Unit:	Scale from 1 to 10		
Criteria:	Low levels of the scale represent low levels of usability while high levels represent a high level of satisfaction on the experience in the use of the tool.		
Relevance:	High relevance. The usability is one of the strong points of the SocIoTal tools.		

KPI Id:	013	KPI title:	% Application crashes
Definition:	Percentage of application crashes during the usage of the Mood of the city enabler		
Unit:	Percentage		
Criteria:	A high percentage of application crashes results in a low performance.		
Relevance:	High relevance. The number of application crashes has to be as lower as possible in order to improve the degree of comfort in the use of the tool.		

KPI Id:	014	KPI title:	Process performance time
Definition:	Time the user takes to provide a data (current image of themselves and answers to the specific question)		
Unit:	Seconds		
Criteria:	Capture the time the user takes to provide a data, i.e. current image of themselves and answers to the specific question. Repeat the process with different kind of users in order to get enough data to perform statistical analysis.		
Relevance:	Medium relevance. The different statistical parameters extracted from the measurement of this KPI (average time, variance, etc.) will show how the tool performance is among different set of users (non-geek users, developers, etc.)		

KPI Id:	015	KPI title:	% Facial expression detection accuracy
Definition:	Percentage of success Facial expression detection accuracy		
Unit:	Percentage		
Criteria:	A high percentage will represent a high level of accuracy of the enabler in real time situation.		
Relevance:	High relevance to assess the correct implementation of the enabler.		

KPI Id:	016	KPI title:	% Environmental data accuracy
Definition:	Percentage of accuracy of environmental data		

Unit:	Percentage
Criteria:	A high percentage will represent a high level of accuracy of the enabler in real time situation.
Relevance:	Medium relevance. Assessment of the data accuracy used for computation of some parameters

KPI Id:	017	KPI title:	Look and feel
Definition:	This KPI tries to measures the look and feel perceived by the users when they receive the results.		
Unit:	Scale from 1 to 10		
Criteria:	Low levels of the scale represent low levels of look and feel perception while high levels represent a high level of satisfaction of the experience in the visualization of results.		
Relevance:	High relevance. As a key of SocIoTal, the user experience has to be as positive as possible.		

2.4.6 Mood Of the City Trial plan

2.4.6.1 Prototypes (enablers & tools) involved development

According to the general trial evaluation process, the different stages, actors and elements involved in the above mentioned functional tools test will be:

1. Prototypes (enablers & tools) involved development: the here described scenarios will test the initial beta versions of the:
    - Data collection tool, that detects users' mood from camera, collect data from environmental sensors and populated questionnaire
    - Mood of the city computation tool, that provide the functionalities to compute final mood of the city index based on input parameters

    These tests will also involve the SocIoTal Context Manager and the selected platform users and resource directories. It will also include, as far as possible and as appropriate, the integration with the SocIoTal Security framework defined within WP2/3 and the Users Environment provided by WP4.

The initially planned time to get the first beta versions to be tested in lab is 5 months within Task 5.2, including also the integrations needed, although some initial works have already started before.

2.4.6.2 Lab Testing

Preliminary testing for Mood of the city field trial will start on M17 and includes testing of beta version of application for:

- application stability (potential crashes, process performance time, etc)
- facial expression detection accuracy
- environmental data accuracy

After beta testing a first alpha version will be provided in order to proceed with a next User Enrolment & Trial deployment phase.

2.4.6.3 Users Enrolment & Trial deployment

Initial enrolment of the users will be initiated when the first stable version of the tool become available. Introduction of the tool and further actions should be done through the IoT Meetups and the different workshops planned during the first half of the second year of SocIoTal, a set of trial users will be selected:

- Final users (standard user profile). Around 30 envisioned participants will test, through the users interface provided, the functionalities and performance of the SocIoTal functional tools.
- Developer Users (geek users/developers profile). Around 20 envisioned participants will directly work with the tool APIs provided, testing the feasibility of these APIs to be integrated within other environments (their own user interfaces).

2.4.6.4 Trial evaluation & Feedback Collection

Evaluation of the trial will be done with two target groups using feedback collected from questionnaires during the workshops. This action will be started on M24 and, during two months, the selected set of users will be provided with the user interfaces and the APIs access needed to perform the different tests that compose this trial. These tests performance will be specified during the lab validation of the prototypes, according the way these developments are built and focused on the KPIs to be collected. A description of the trial, the steps and all info needed to play them will be provided to participants before the trial starts.

2.4.6.5 Corrective & Improvements actions

Using identified KPIs for this field trial feedback will be collected about application usability, application stability (potential crashes, process performance time, etc), facial expression detection accuracy, environmental data accuracy, and its looks and feel. The KPIs evaluation will result with a feedback that will require a following corrective and improvement action for possible emerged issues:

- Correction of detected bugs
- Improvement of components' usability
- Improvement of components performance/efficiency

This set of stages describing the trials evaluation performance will be distributed mainly along the second year of the SocIoTal project, starting officially on M16 and ending on M27, led by Task 5.2 of the project. An example of the planning presented in next trials specifications is shown in Figure 12.

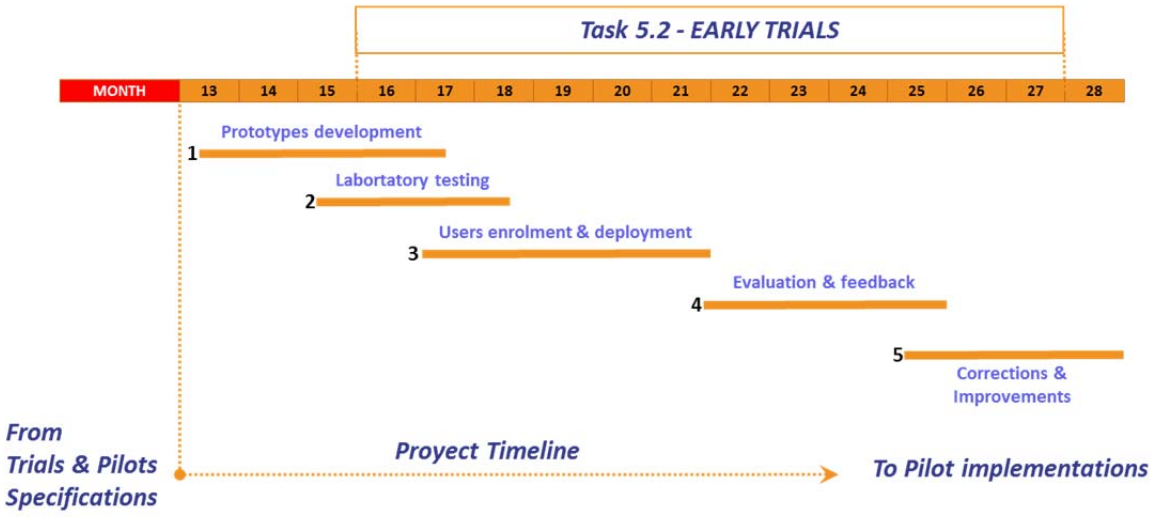

Figure 12. Timeplan for Mood of the city field trial

2.5 Evaluating Elevator Supervisor

One of the challenges tenants have from time to time is building maintenance, more specifically elevator repairs. There is no efficient method to know which distance elevator reaches between scheduled inspections, thus this number can be significantly different in the same time intervals. To provide better insight into these numbers, as well as to provide automatic detection of elevator malfunction elevator supervisor use case is proposed.

This trial will evaluate elevator supervisor deployment that enables tenants to monitor history of repairs, elevator distance travelled between inspections and to signal when a new repair is required, as well as to detect malfunction. SocIoTal Environment Web application [8] portal can be used to add new users that can monitor elevator condition, schedule next inspection depending on number of travelled kilometres, put alarms for elevator jams and inspections.

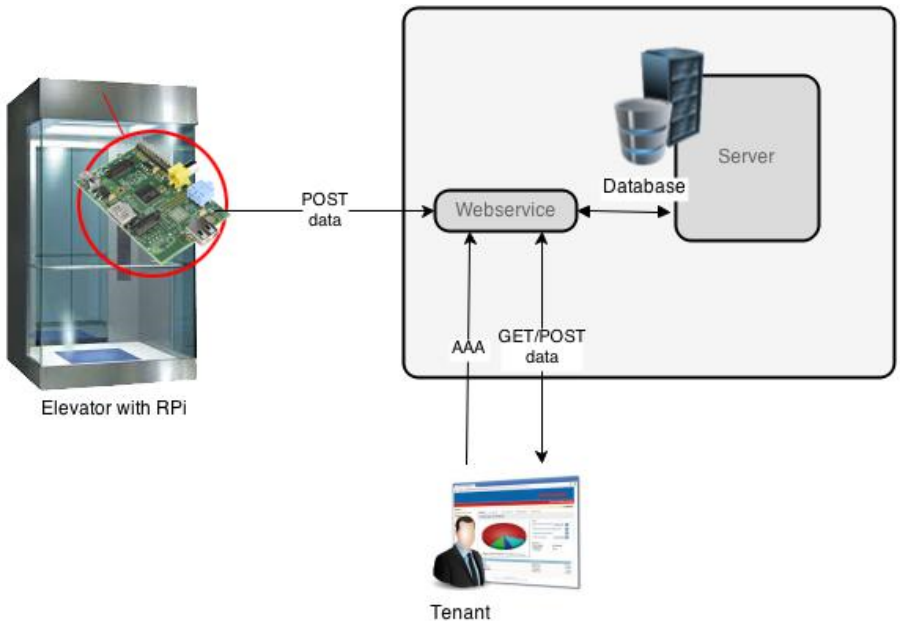

Figure 13. Data flow for Elevator supervisor use case

2.5.1 Scenario 3-2: Elevator supervisor

A chief tenant was intending to log in SocIoTal web portal that enables him to monitor details about the elevator in his building. But, just before he logged in, he got an email alert that inspection is required as elevator will soon reach a next distance target point for routine check.

2.5.2 Use Case 3-2.1: Detecting elevator's travelled distance

This use case is based on a set of HW and SW tools that enable monitoring of elevator travelled distance. Raspberry Pie (RPi) device [9] with accelerometer is used to detect movements and after postposing of the signal using low pass filter a number of travelled meters is calculated and sent to the SocIoTal Web application. Users can track travelled distance of the elevator in order to schedule an elevator inspection.

2.5.3 Use Case 3-2.2: Detecting elevator malfunction

This use case is used to automatically detect elevator malfunction by using accelerometers' and PIR sensor [10] data attached on the RPi board. If detected, details about malfunction are sent to the SocIoTal Web portal. User can create notifications in case of malfunction in order to be alerted in case of emergency.

2.5.3.1 List of Key Performance Indicators (KPI)

This section presents a set of tables which shows the Key Performance Indicators selected for the trial of the elevator supervisor These KPIs will cover different aspects such as the number of users to evaluate the trial, their perceptions or technical KPIs as enabler malfunctions among others. These tables describe an identifier for the KPI, its name, a definition, the unit of measure, the criteria followed for the evaluation, and the relevance of the KPI compared to the other measurements in the list.

KPI Id:	001	KPI title:	Number of evaluators
Definition:	Number of people from the target groups that will evaluate the elevator supervisor enabler.		
Unit:	Number of people		
Criteria:	The greater the number of people who evaluate the trial, greater the success of the KPI. Depending on the evaluation phase the correspondent target group will be selected.		
Relevance:	Medium relevance. It is not considered as high relevance because even if there are not many people involved in the evaluation it can be successful if the most failures and interesting improvements are discovered.		

KPI Id:	017	KPI title:	Look and feel
Definition:	This KPI tries to measures the look and feel perceived by the users when they receive the results.		
Unit:	Scale from 1 to 10		
Criteria:	Low levels of the scale represent low levels of look and feel perception while high levels represent a high level of satisfaction of the experience in the visualization of results.		
Relevance:	High relevance. As a key of SocIoTal, the user experience has to be as positive as possible.		

KPI Id:	018	KPI title:	Usability
Definition:	Usability measures the grade of simplicity perceived by users when they use elevator		

	supervisor application.
Unit:	Scale from 1 to 10
Criteria:	Low levels of the scale represent low levels of usability while high levels represent a high level of satisfaction on the experience in the use of the tool.
Relevance:	High relevance. The usability is one of the strong points of the SocIoTal tools.

KPI Id:	019	KPI title:	% Application crashes
Definition:	Percentage of application crashes during the usage of the elevator supervisor enabler		
Unit:	Percentage		
Criteria:	A high percentage of application crashes results in a low performance.		
Relevance:	High relevance. The number of application crashes has to be as lower as possible in order to improve the degree of comfort in the use of the tool.		

KPI Id:	020	KPI title:	% Malfunction detection accuracy
Definition:	Percentage of success of malfunction detection accuracy		
Unit:	Percentage		
Criteria:	A high percentage will represent a high level of accuracy of the enabler in real time situation.		
Relevance:	High relevance to assess the correct implementation of the enabler.		

KPI Id:	021	KPI title:	% Travelled distance calculation accuracy
Definition:	Percentage of success of travelled distance calculation accuracy		
Unit:	Percentage		
Criteria:	A high percentage will represent a high level of accuracy of the enabler in real time situation.		
Relevance:	High relevance to assess the correct implementation of the enabler.		

2.5.4 Evaluator Supervisor Trial plan

2.5.4.1 Prototypes (enablers & tools) involved development

According to the general trial evaluation process, the different stages, actors and elements involved in the above mentioned functional tools test will be:

2. Prototypes (enablers & tools) involved development: the here described scenarios will test the initial beta versions of the:

    - Distance computation tool, that provide the detect elevator travelled distance based on sensor readings and data processing

    - Elevator malfunction detection tool, that enables automatic detection of elevator malfunction and notification of a predefined group of users using SocIoTal Web application defined and developed within WP4.

    In order to perform the security actions needed to identify and authenticate the coming requests (data, membership, modifications, etc.). Interactions with the Identity Manager (IdM), Group Manager (GM) and Access Control (AC) element will be required. These tests will also involve the SocIoTal Context Manager, SocIoTal Context Broker and the selected platform

users. It will also include, as far as possible and as appropriate, the integration with the SocIoTal Security framework defined within WP2/3 and the Users Environment provided by WP4.

The initially planned time to get the first beta versions to be tested in lab is 5 months within Task 5.2, including also the integrations needed, although some initial works have already started before.

2.5.4.2 Lab Testing

Preliminary testing this field trial will start on M17 and includes testing of beta version of application for:

- application stability (potential crashes, process performance time, etc)
- facial expression detection accuracy
- environmental data accuracy

After beta testing a first alpha version will be provided in order to proceed with a next User Enrolment & Trial deployment phase.

2.5.4.3 Users Enrolment & Trial deployment

Initial enrolment of the users will be initiated when the first stable version of the tool become available. Introduction of the tool and further actions should be done through the IoT Meetups and the different workshops planned during the first half of the second year of SocIoTal, a set of trial users will be selected:

- Final users (standard user profile). Around 30 envisioned participants will test, through the users interface provided, the functionalities and performance of the SocIoTal functional tools.
- Developer Users (geek users/developers profile). Around 20 envisioned participants will directly work with the tool APIs provided, testing the feasibility of these APIs to be integrated within other environments (their own user interfaces).

2.5.4.4 Trial evaluation & Feedback Collection

Evaluation of the trial will be done with two target groups using feedback collected from questionnaires during the workshops. This action will be started on M24 and, during two months, the selected set of users will be provided with the user interfaces and the APIs access needed to perform the different tests that compose this trial. These tests performance will be specified during the lab validation of the prototypes, according the way these developments are built and focused on the KPIs to be collected. A description of the trial, the steps and all info needed to play them will be provided to participants before the trial starts.

2.5.4.5 Corrective & Improvements actions

Using identified KPIs for this field trial feedback will be collected about application usability, application stability (potential crashes, process performance time, etc), travelled distance accuracy, malfunction detection efficiency, and its looks and feel. The KPIs evaluation will result with a feedback that will require a following corrective and improvement action for possible emerged issues:

- Correction of detected bugs
- Improvement of components' usability
- Improvement of components performance/efficiency

The feedback collection (to get suggestions, improvements and so on) is expected to start providing valuable information during the second half of the stage 4. This time, the evaluation of these initial set of corrections, suggestions and improvements will be evaluated by DNET developers in order to implement as far as possible those relevant ones, to be available for the pilots.

This set of stages describing the trials evaluation performance will be distributed mainly along the second year of the SocIoTal project, starting officially on M16 and ending on M27, led by Task 5.2 of the project. An example of the planning presented in next trials specifications is shown in Figure 14.

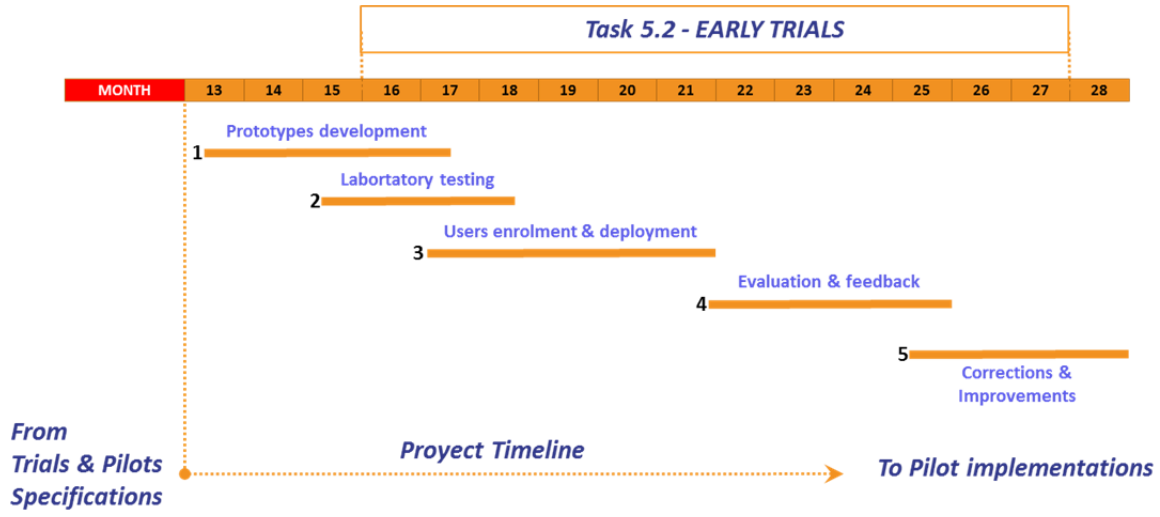

Figure 14. Timeplan for Elevator supervisor field trial

2.6 F2F Enabler evaluation and Real-social graph construction (UNIS)

The F2F Enabler allows discovering and detecting users' social relations through their real-world social interactions, as perceived in their daily life by user mobile smartphone. The social interaction detection is achieved by combining two different types of information, users' relative orientation and users' interpersonal distance Figure 15.

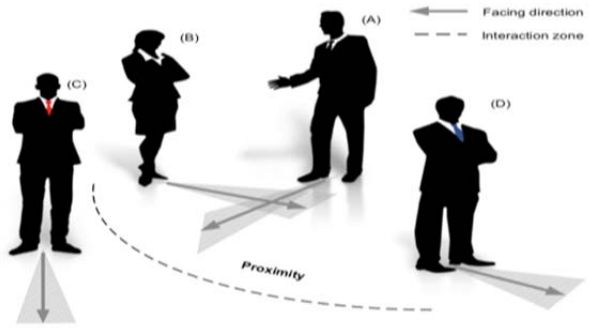

Figure 15. F2F enabler overview

According to Hall [11] distance at which users interact can be seen as expression of their social relations. Figure 15 shows an overview of the different situation the F2F enabler is able to capture, with only subjects A and B recognised as involved in an actual social relation.

Aim of this trial is to evaluate the effectiveness of the proposed F2F enabler and its integration with the SocIoTal framework in order to extract actual F2F relations and its accuracy to provide large scale information to build a social graph as detected by real users' interactions. The extracted information will later support creation of specific bubble and community and the detection of specific context [12].

2.6.1 Scenario 4-1

The trial aims to validate the TRL (Technology Readiness Level) of the F2F enabler. Aim of this trial is to allow participants to measure their daily F2F interaction through their mobile phones and to review the real social graph that they build during their day, through a provided mobile application integrating relevant SocIoTal tools. End-user participants will be recruited for this trial. Participants following a regular life, that alternates between work, social and home time, will be preferred. On the other end, in a second phase, developers, either expert or passionate about IoT security, will be also recruited in order to challenge the security of the F2F technology.

Students in the University of Surrey Campus and Researchers at the Institute for Communication Systems will be also enrolled, together with citizens and other people attending SOCIOTAL meetups. For a small group of people, representing the *focus group* some mobile phone can be also provided as part of incentive to participate to the experiment. In addition, the possibility to recruit participants in the third-party partner city of Taipei in a Retail environment to detect the relationships between customers and their relative location in the shops will be investigated.

2.6.2 Use case 4-1.1. F2F accuracy validation

User will be asked to carry their mobile phone with them most of the time, conduct a normal life and to interact with the provided application. The application will run in background and will try to detect F2F interactions. As soon as a F2F interaction is detected, and the knowledge about it is extracted, the guessed interaction type will be prompted to the user on their mobile phone screen, using a notification system. The user will be allowed to set up the frequency of notification received by the app and the number of F2F interaction he/she agrees to rate per day. Collected information will be acquired and stored in the SocIoTal server for further progressing.

2.6.3 Use case 4-1.2. F2F privacy level validation

The application using the F2F technology will be integrated with existing tools, such as the USEMP [12] tool for privacy monitoring and the IoT Lab [13] for feedback collection. As one of the features of the application is to extract F2F social relation information in a privacy preserving fashion, by performing computation at device level and without leaking any information sharing outside of the device, the USEMP tools will allow to monitor the shared information and to prompt such information to the user. At the end of the experiment the users will be prompted with a USEMP daily report and asked to rate their degree of perceived privacy in using the app and comfort with the experiment and proposed technology. Collected information will be acquired and stored in the SocIoTal server for further progressing.

2.6.4 Use case 4-1.3. Creation of real social graphs

In addition, in order to benchmark real social graph created through detected F2F interactions with social graphs extracted from social networks (e.g., Twitter, Facebook and other) at the end of an experiment, volunteer participants will be asked to review their real social graphs, as extracted by the

collected data and generated by the SocIoTal server, under the agreement to share information about their social graphs as obtained from their social network profiles.

2.6.5 Use case 4-1.4. F2F security level validation

At the end an experiment phase, developers willing to challenge the F2F enabler will submit a report composed of at least the following information: time stamp, detected type F2F relation, involved devices. The data will be used to compute relevant KPIs quantifying the security level of the F2F technology, by measuring the number of unauthorized F2F relations detected.

2.6.5.1 List of Key Performance Indicators (KPI)

This section presents a set of tables which shows the Key Performance Indicators selected for the trial of the F2F enabler.

KPI Id:	001	KPI title:	Number of evaluators
Definition:	Number of people from the target groups that will evaluate the F2F enabler.		
Unit:	Number of people		
Criteria:	The greater the number of people who evaluate the trial, greater the success of the KPI.		
Relevance:	Medium relevance. It is not considered as high relevance because even if there are not many people involved in the evaluation it can be successful if the most failures and interesting improvements are discovered.		

KPI Id:	022	KPI title:	% of rated F2F interactions
Definition:	Percentage of detected interactions that have been rated by evaluators.		
Unit:	Ratio		
Criteria:	The greater the number of rated interactions with respect to the detected ones greater the success of the KPI.		
Relevance:	High relevance. An higher ratio is indication of high participation and interest for the proposed technology		

KPI Id:	023	KPI title:	% of shared social profiles
Definition:	Percentage of participants willing to share information about their social profiles.		
Unit:	Ratio		
Criteria:	The greater the number of shared social profiles with respect to the number of participants greater the success of the KPI.		
Relevance:	High relevance. An higher ratio is indication of high participation and interest for the proposed technology		

KPI Id:	024	KPI title:	User trust
Definition:	User trust measures the grade of trust perceived by users in utilizing the app and checking the type of shared information		
Unit:	Scale from 1 to 10		
Criteria:	Low levels of the scale represent low levels of trust while high levels represent a high level of trust on the experience in the use of the app.		
Relevance:	High relevance. The perceived trust is one of the strong points of the SocIoTal F2F enabler.		

KPI Id:	025	KPI title:	% Correct detected interactions

Definition:	Percentage of success occurred between system detected F2F relation and user rated one
Unit:	Percentage
Criteria:	A high percentage will represent a high level of accuracy of the enabler in real time situation.
Relevance:	High relevance to assess the correct implementation of the enabler.

KPI Id:	026	KPI title:	% Energy spent
Definition:	Percentage of energy consumed by the app with respect to other app energy during the trial duration.		
Unit:	Percentage		
Criteria:	A high percentage of energy results in a low performance and possibly a mistrust of the user toward the app.		
Relevance:	High relevance. A low energy consumption of the app is indication of an effective implementation of it and the possibility for the tool to be well received by the users.		

KPI Id:	027	KPI title:	% Data spent
Definition:	Percentage of data traffic generated by the app with respect to other app data traffic during the trial duration.		
Unit:	Percentage		
Criteria:	A high percentage of data traffic results in a low performance and possibly a mistrust of the user toward the app.		
Relevance:	High relevance. A low data traffic generated by the app is indication of an effective implementation of it and the possibility for the tool to be well received by the users.		

KPI Id:	028	KPI title:	% Leaked F2F relations
Definition:	Percentage of leaked F2F relation detected by a malicious device with respect to the authorized genuine ones collected by the SOCIOTAL platform.		
Unit:	Percentage		
Criteria:	A high percentage of leaked F2F relations results in a low performance and security level of the technology.		
Relevance:	High relevance. A low percentage of leaked F2F relations is indication of an effective implementation of it and the possibility that the enabler will be hard to tamper.		

2.6.6 Trial plan

2.6.6.1 Prototypes (enablers & tools) involved development

The F2F enabler will be finalized by M18, including integration of security mechanism that prevent the devices running the enabler against the most common privacy attacks (e.g., impersonification and spoofing). In addition the final prototype for testing will require the implementation of i) mechanisms to increase resilience of the enabler in estimating interpersonal distance, when variations of the Received Signal Strength Indication (RSSI) due to the environment are present; ii) solution to increase the accuracy in estimating the facing direction when device displacements occur. This phase will end in M18.

2.6.6.2 Lab Testing

Experiments similar to those described in [14] will be performed in a small scale (4/5 participants) in a controlled lab environment to test the improved beta version of the F2F mobile application. In particular the following will be tested:

- Accuracy in detecting facing direction and distance estimation in different conditions and environment;
- Accuracy and resilience of the F2F detection depending on the used mobile phone;

After beta testing a first alpha version will be provided in order to proceed with a next User Enrolment & Trial deployment phase. It is expected that this phase will last one month and end in M19.

2.6.6.3 Users Enrolment & Trial deployment

The F2F enabler will be integrated with other enablers and SocIoTal components in order to support the different experimentation phases. The integration with the following components is envisioned:

- Integration with the SocIoTal Authentication component to support user registration;
- Integration with the SocIoTal Context Manager and in particular its communication module (Context Broker) to share the collected face-to-face interaction data;
- Potentially integration (subject to component availability) with the EU IoT Lab and USEMP project tools to support the collection of feedback from users and KPIs computation;
- Integration with Facebook, Twitter, GooglePlus APIs, to access user social graph upon user consent;

In parallel, the different selected sets of trial users and developers will be engaged and introduced to the trials enabler, functionalities and objectives. Initially a first smaller group of user participants will be recruited in the ICS (Institute for Communication Systems) at the University of Surrey, by running a dedicated information event. For larger experiments, presentation of the trial will be made in dedicated meetup event, along with the possibility to push recruitment campaigns through the University of Surrey QR-code/NFC tag points and Smart Display infrastructure. In particular when somebody in the campus interact with such devices, could be exposed to the F2F technology presentation and asked to participate to experiment. This phase will take about three months and is expected to end in M21.

2.6.6.4 Trial evaluation & Feedback Collection

Evaluation of the trial will be performed in two rounds with two target groups and evaluated by using both the collected in-app data and other feedback collected from questionnaires/surveys, ideally distributed within the app. The surveys will focus on collecting input from user experience, perceived degree of privacy and other metric useful for the computation of KPIs presented in Section 2.6.5.1. Details about the experiment duration are reported in 0. It is envisioned that two main trials will take place involving initially citizens in the number of respectively 10 and 30 participants and only in the second phase developers, with the main target to challenge the provided implementation from a security point of view. In addition, in each trial the required interaction with the participants might

differ, as survey and extensive data collection will be performed in different phases. This phase will take place in M22-M25.

2.6.6.5 Corrective & Improvements actions

After the envisioned trials are performed, using the collected information, identified KPIs will be computed and results analysed. Other than aspects related to application usability, application stability (potential crashes, process performance time, etc), F2F detection accuracy, implementation security and efficiency that will allow to create a more stable version of the application to be used in large pilots with end users and potentially to solution exploited further after the SocIoTal project, other research insights are expected to be collected and extracted from the planned trials. The KPIs evaluation will result with a feedback that will require a following corrective and improvement action for possible emerged issues:

- Correction of detected bugs
- Improvement of components' usability
- Improvement of components performance/efficiency

This set of correction will be performed between M26 and M27 when the application will be finally available for larger city pilots.

This set of stages describing the trials evaluation performance will be distributed mainly along the second year of the SocIoTal project, starting officially on M16 and ending on M27, led by Task 5.2 of the project. While final implementation of the enabler will continue until the end of the Task, however the trials are expected to be finished and data analysed in M25 in order to be described into D5.2. [15]. An example of the planning described above is shown in Figure below.

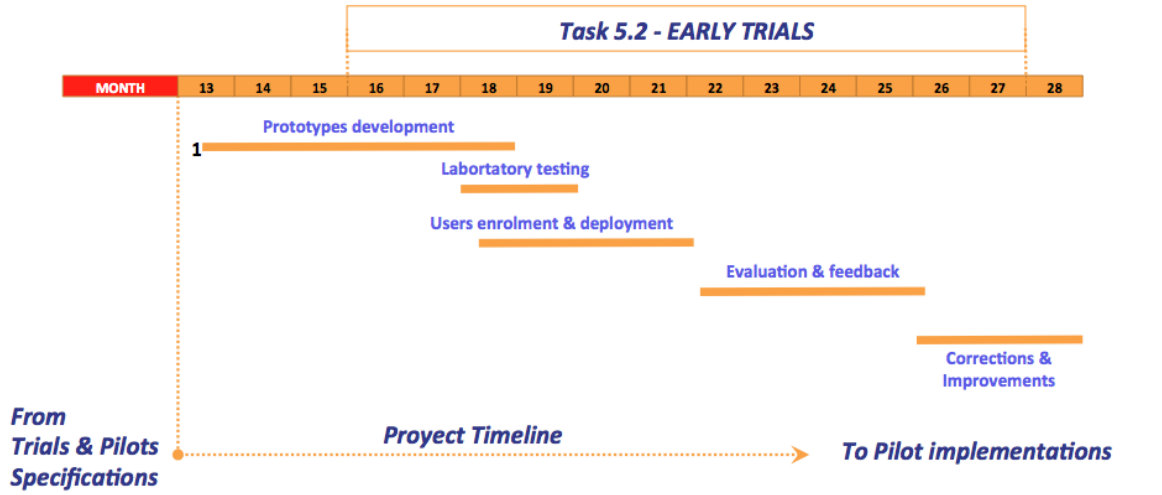

Figure 16. Timeplan for F2F enabler trial

2.7 Evaluating of Privacy-preserving reputation and discovery (UNIS)

Privacy-Preserving discovery and data sharing tools allows users who participate to SocIoTal to share data generated by their devices, (e.g., mobile phones) only if requested data fulfil user privacy settings. Using a distributed anomaly detection algorithm running on user devices, reputation scores can be assigned to data sources associated to the device. This can be done in a privacy-preserving fashion without need to share raw data coming from user devices with external SocIoTal tools, but by relaying metadata from the devices using a distributed algorithm. After a reputation score is assigned to the devices, by for instance comparing the quality of the data generated by the selected device, with the data generated by infrastructure and well-calibrated devices, this score will be stored in the device.

Once data are required in a given location, where no infrastructure device are available, the SocIoTal Broker (Figure 17) will advertise the requirement to SocIoTal participating devices and mobile phones about the type of required data and their location. If devices with a good reputation score can match the required position, and internal sharing policies will allow to share such data (or explicit consent is given by the user), in the required context, the data provided will start to flow into the requesting SocIoTal devices. The mechanism is privacy-preserving as no raw device data is shared to build the reputation score and no raw device data are shared with the system if no consent is given (either manually or through well-defined policies).

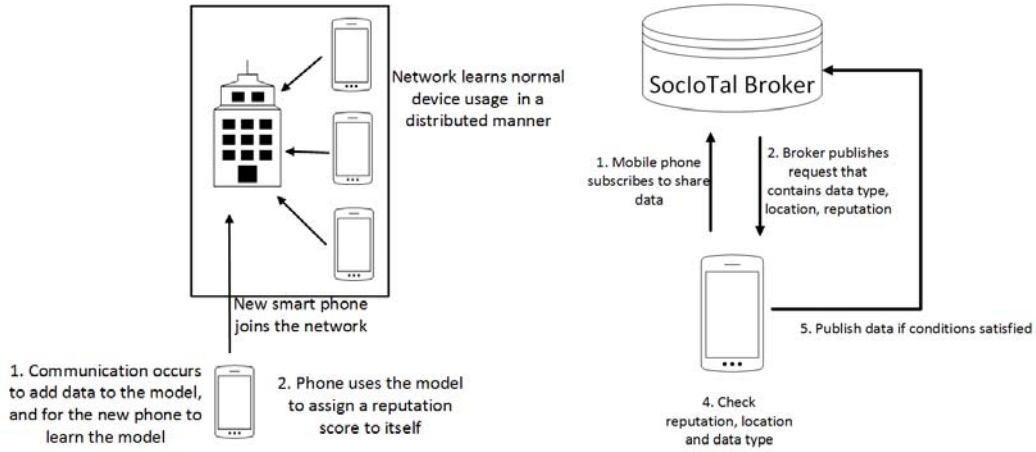

Figure 17. Privacy-aware discovery - reputation computation (left), privacy-aware discovery (right)

2.7.1 Scenario 4-2

Aim of this trial is to allow participants to share the data generated by their mobile phone towards requesting devices for the creation of citizen-centric service in a privacy preserving way. In addition, the trial aims to monitor and rate the level of privacy perceived by the user through a provided mobile application integrating relevant SocIoTal tools. End-user participants will be recruited for this trial. Participants following a regular life, that alternates between work, social and home time, will be preferred. Users should spend a portion of their life in areas where sensing infrastructure owned by the SocIoTal project is deployed, such as Santander city and University of Surrey campus. Developers aiming at challenging the proposed enabler will also be involved. Participants will be recruited in a similar way and through similar channels as described in Section 2.6.1.

2.7.2 Use case 4-2.1. Reputation score computation

User will be asked to carry their mobile phone with them most of the time, conduct a normal life and to interact with the application. The application will run in background and will first assess the reputation score of the device, when the user device is in presence of fixed sensing infrastructure. In this case the device will exchange metadata (either directly or through gateway, depending on the characteristics of the present infrastructure) with infrastructure devices. No actions are required to the user at this stage.

2.7.3 Use case 4-2.2. Privacy-preserving discovery evaluation

Subsequently, when the device has computed its reputation score, it will be able to satisfy data sharing requests. To this purpose, when the user moves in different locations then app will start to satisfy request for data sharing coming from the SocIoTal Broker. As soon as request for data than can be satisfied by the device is detected (i.e., matching location, data type and reputation score), the decision will be prompted to the users on their mobile phone screen, using a notification system, and consent to share the data will be asked. The user will be allowed to set up the frequency of notification received by the app and the number of data sharing he/she agrees to rate per day. Collected information will be acquired and stored in the SOCIOTAL server for further progressing.

2.7.4 Use case 4-2.3. Enabler privacy level validation

Similarly to what described for the F2F enabler evaluation, USMEP [12] and IoT Lab [13]. Tools will be integrated in supporting the trial (Section 2.7.2). At the end of the experiment, users will be asked to rate their degree of perceived privacy in using the application and comfort with the experiment and proposed technology.

2.7.5 Use case 4-2-4. Enabler security level validation

At the end an experiment phase, developers willing to challenge the Privacy-preserving discovery enabler will submit a report composed of at least the following information: time stamp, involved devices, type and value of leaked device data. The information will be used to compute relevant KPIs quantifying the security level of the enabler, by measuring the number of unauthorized leaked device data.

2.7.5.1 List of Key Performance Indicators (KPI)

This section presents a set of tables which shows the Key Performance Indicators selected for the trial of the Privacy-preserving reputation and discovery enabler.

KPI Id:	001	KPI title:	Number of evaluators
Definition:	Number of people from the target groups that will evaluate the enabler.		
Unit:	Number of people		
Criteria:	The greater the number of people who evaluate the trial, greater the success of the KPI.		
Relevance:	Medium relevance. It is not considered as high relevance because even if there are not many people involved in the evaluation it can be successful if the most failures and interesting improvements are discovered.		

KPI Id:	024	KPI title:	User trust
Definition:	User trust measures the grade of trust perceived by users in utilizing the app and checking the type of shared information		
Unit:	Scale from 1 to 10		
Criteria:	Low levels of the scale represent low levels of trust while high levels represent a high		

	level of trust on the experience in the use of the app.
Relevance:	High relevance. The perceived trust is one of the strong points of the SOCIOTAL privacy-preserving enabler.

KPI Id:	026	KPI title:	% Energy spent
Definition:	Percentage of energy consumed by the app with respect to other app energy during the trial duration.		
Unit:	Percentage		
Criteria:	A high percentage of energy results in a low performance and possibly a mistrust of the user toward the app.		
Relevance:	High relevance. A low energy consumption of the app is indication of an effective implementation of it and the possibility for the tool to be well received by the users.		

KPI Id:	027	KPI title:	% Data spent
Definition:	Percentage of data traffic generated by the app with respect to other app data traffic during the trial duration.		
Unit:	Percentage		
Criteria:	A high percentage of data traffic results in a low performance and possibly a mistrust of the user toward the app.		
Relevance:	High relevance. A low data traffic generated by the app is indication of an effective implementation of it and the possibility for the tool to be well received by the users.		

KPI Id:	029	KPI title:	Number of rated discovery procedures
Definition:	Number of discovery procedures that have been rated by evaluators.		
Unit:	Ratio		
Criteria:	The greater the number of rated procedures with respect to the detected ones greater the success of the KPI.		
Relevance:	High relevance. An higher ratio is indication of high participation and interest for the proposed technology		

KPI Id:	030	KPI title:	% Correct detected discoveries
Definition:	Percentage of success occurred between system detected discoveries and user rated one		
Unit:	Percentage		
Criteria:	A high percentage will represent a high level of accuracy of the enabler in real time situation in sharing data in context the user agree to share them		
Relevance:	High relevance to assess the correct implementation of the enabler.		

KPI Id:	031	KPI title:	% Leaked device data
Definition:	Percentage of leaked device data detected by a malicious device with respect to the authorized data collected and shared by the SOCIOTAL platform.		
Unit:	Percentage		
Criteria:	A high percentage of leaked device data results in a low performance and security level of the technology.		
Relevance:	High relevance. A low percentage of leaked device data is indication of an effective implementation of the enabler and the possibility that the enabler will be hard to		

	tamper.

2.7.6 Trial plan

2.7.6.1 Prototypes (enablers & tools) involved development

The Privacy-preserving discovery enabler will be finalized by M21, by implementing a prototype working on mobile phones and other sensor mote platforms. In addition the final prototype for testing will require the development and implementation able to cope with the addition of new devices into an existing sensor network, i.e., arrival and departure of other mobile phones providing crowdsensing capabilities. This phase will terminate in M21.

2.7.6.2 Lab Testing

A small-scale replica of the experiment described in Section 2.7.2 will be performed in a controlled lab environment, including 1 or 2 participants. In particular the ability of the mobile phone implementation of the algorithm to compute its reputation score accordingly to the identified outliers will be tested and validated.

After beta testing a first alpha version will be provided in order to proceed with a next User Enrolment & Trial deployment phase. It is expected that this phase will last one month and end in M22.

2.7.6.3 Users Enrolment & Trial deployment

In this phase, the Privacy-preserving discovery enabler will be integrated with other enablers and SocIoTal components in order to support the different experimentation phases. The integration with the following components is envisioned:

- Integration with the SocIoTal Authentication component to support user registration;
- Integration with the SocIoTal Context Manager and in particular its communication module (Context Broker) to share the collected meta-data for reputation computation and request for data sharing;
- Potentially integration (subject to component availability) with the EU IoT Lab and USEMP project tools to support the collection of feedback from users and KPIs computation;

In parallel, the different selected sets of trial users and developers will be engaged and introduced to the trials enabler, functionalities and objectives. A recruitment procedure similar to the one described in Section 2.6.6.3 will be performed. This phase will take about two months and is expected to end in M24.

2.7.6.4 Trial evaluation & Feedback Collection

Evaluation of the trial will be performed in two rounds with short experiments each and two target groups and evaluated by using both the collected in-app data and other feedback collected from questionnaires/surveys, ideally distributed within the app. The surveys will focus on collecting input from user experience, perceived degree privacy and other metric useful for the computation of KPIs presented in Section 2.7.5.1. Details about the experiment duration are reported in Table 1. It is envisioned that two main trials will be performed involving initially citizens in the number of respectively 10 and 30 participants and developers in the number of 5 to 10, with the main target to

challenge the provided implementation from a security point of view and to develop new services using the provided enabler. This phase will take place in M24-M25.

2.7.6.5 Corrective & Improvements actions

After the envisioned trials are performed, using the collected information, identified KPIs will be computed and results analysed. Aspects related to application usability, application stability (potential crashes, process performance time, etc), reputation algorithm accuracy, implementation security and efficiency will be considered. In addition, to information that will allow to create a more stable version of the application to be used in large pilots with end users and potentially to solution exploited further after the SocIoTal project, other research insights are expected to be collected and extracted from the planned trials. The KPIs evaluation will result with a feedback that will require a following corrective and improvement action for possible emerged issues:

- Correction of detected bugs
- Improvement of components' usability
- Improvement of components performance/efficiency

This set of correction will be performed between M26 and M27 when the application will be finally available for larger city pilots.

This set of stages describing the trials evaluation performance will be distributed mainly along the second year of the SocIoTal project, starting officially on M16 and ending on M27, led by Task 5.2 of the project. While final implementation of the enabler will continue until the end of the Task, however the trials are expected to be finished and data analysed in M25 in order to be described into [15]. An example of the planning described above is shown in Figure below.

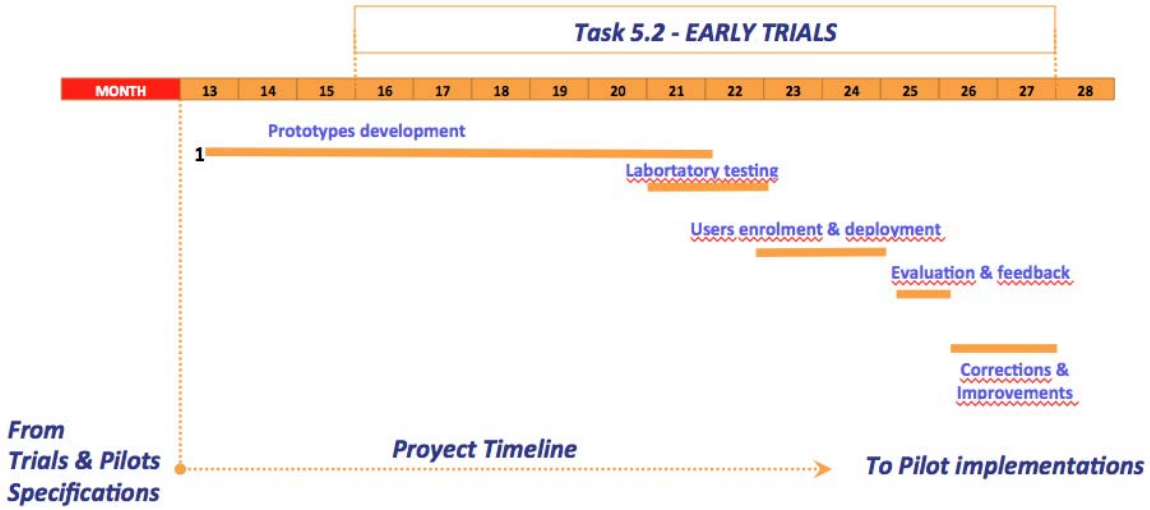

Figure 18. Timeplan for Privacy-preserving discovery enabler trial

2.8 Evaluating of User Trust Tools (UNIS)

The Trust tool is a tool that allows to classify a device (e.g., mobile phone) based on the following question: is the phone is used by its normal user? This can be achieved by extracting a user footprint coming from different sensor streams collected from the user devices and identifying anomalies when a deviation from the user normal behaviour is detected. The tool can be used to identify malicious users of the SocIoTal platform or to annotate genuine data when authentic data are shared and the device acts as data source. This could prevent the user for signing up him/her and his/her device to the SocIoTal platform using user/name and password, thus guaranteeing anonymity. Additionally, as the proposed solution will run in a distributed manner on the user device, its privacy-preserving aspects are guaranteed.

Figure 19 shows how the Trust tool locally uses only information extracted from the user mobile phone without sharing of collected data. The SocIoTal enabler will then generate alert when *Not Authorized* usage is detected by sharing this information as part of the detected context when interacting with the SocIoTal Broker. The other SocIoTal Security components will manage the alarm accordingly.

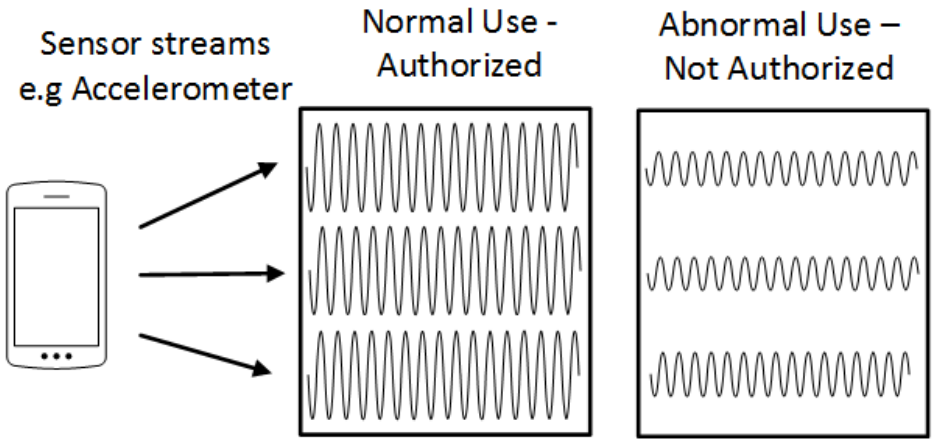

Figure 19. User trust tool

2.8.1 Scenario 4-3

Aim of this trial is to allow participants to verify that their mobile phone has not been used by non-authorized users through the use and test of a provided mobile application featuring relevant SocIoTal tools. End-user participants will be recruited for this trial. Participants following a regular life, that alternates between work, social and home time, will be preferred. In addition, developers willing to challenge the security of the enabler will be also recruited. Participants will be recruited in a similar way and through similar channels as described in Section 2.7.1.

2.8.2 Use case 4-3.1. Trust tool evaluation

User will be asked to carry their mobile phone with them most of the time, conduct a normal life and to interact with the application. The application will run in background and will first create a footprint for user identification, then it will start to monitor occurrence of anomalies and identify change of user or usage conditions. At some point the user will be required to perform different action from his/her normal behaviour, through a dedicated notification channel, and as soon the anomaly is detected by the system the decision will be prompted to the users on their mobile phone screen, requiring for user annotation of the correct detection. A user participation similar to the other use case described above will be required. The user will be allowed to set up the frequency of notification

received by the application and the number of actions he/she agreed to perform to change its behaviour. Collected information will be acquired and stored in the SocIoTal server for further processing.

2.8.3 Use case 4-3.2. Trust tool privacy level evaluation

Similarly to what described for the F2F enabler evaluation, USMEP [12] and IoT Lab [13] tools will be integrated in supporting the trial (Section 2.7.2). At the end of the experiment user will be asked to rate their degree of perceived privacy in using the app and comfort with the experiment and proposed technology.

2.8.4 Use case 4-3.3. Trust tool security level evaluation

Developers willing to challenge the security level of the Trust tool will allowed to access the Trust tool mobile app and to use it to perform access to the SocIoTal platform. At the end of an experiment phase they will submit a report composed of at least the following information: time stamp, type of access performed, success or not. The information will be used to compute relevant KPIs quantifying the security level of the enabler, by measuring the number of unauthorized access successfully performed.

2.8.4.1 List of Key Performance Indicators (KPI)

This section presents a set of tables which shows the Key Performance Indicators selected for the trial of the User Trust tool.

KPI Id:	001	KPI title:	Number of evaluators
Definition:	Number of people from the target groups that will evaluate the enabler.		
Unit:	Number of people		
Criteria:	The greater the number of people who evaluate the trial, greater the success of the KPI.		
Relevance:	Medium relevance. It is not considered as high relevance because even if there are not many people involved in the evaluation it can be successful if the most failures and interesting improvements are discovered.		

KPI Id:	024	KPI title:	User trust
Definition:	User trust measures the grade of trust perceived by users in utilizing the app and checking the type of shared information		
Unit:	Scale from 1 to 10		
Criteria:	Low levels of the scale represent low levels of trust while high levels represent a high level of trust on the experience in the use of the app.		
Relevance:	High relevance. The perceived trust is one of the strong points of the SOCIOTAL privacy-preserving enabler.		

KPI Id:	026	KPI title:	% Energy spent
Definition:	Percentage of energy consumed by the app with respect to other app energy during the trial duration.		
Unit:	Percentage		
Criteria:	A high percentage of energy results in a low performance and possibly a mistrust of the user toward the app.		
Relevance:	High relevance. A low energy consumption of the app is indication of an effective		

	implementation of it and the possibility for the tool to be well received by the users.

KPI Id:	027	KPI title:	% Data spent
Definition:	Percentage of data traffic generated by the app with respect to other app data traffic during the trial duration.		
Unit:	Percentage		
Criteria:	A high percentage of data traffic results in a low performance and possibly a mistrust of the user toward the app.		
Relevance:	High relevance. A low data traffic generated by the app is indication of an effective implementation of it and the possibility for the tool to be well received by the users.		

KPI Id:	032	KPI title:	Number of rated anomalies
Definition:	Number of discovery procedures that have been rated by evaluators.		
Unit:	Ratio		
Criteria:	The greater the number of rated procedures with respect to the detected ones greater the success of the KPI.		
Relevance:	High relevance. An higher ratio is indication of high participation and interest for the proposed technology		

KPI Id:	033	KPI title:	% Correct detected anomalies
Definition:	Percentage of success occurred between system detected anomalies and user rated one		
Unit:	Percentage		
Criteria:	A high percentage will represent a high level of accuracy of the enabler in real time situation in detecting malicious users		
Relevance:	High relevance to assess the correct implementation of the enabler.		

KPI Id:	034	KPI title:	% of unauthorized access
Definition:	Percentage of unauthorized access performed by a malicious device with respect to the number of attempted ones.		
Unit:	Percentage		
Criteria:	A high percentage of unauthorized access results in a low performance and security level of the technology.		
Relevance:	High relevance. A low/zero percentage of unauthorized access is indication of an effective implementation of the enabler and the possibility that the enabler will be hard to tamper.		

2.8.5 Trial plan

2.8.5.1 Prototypes (enablers & tools) involved development

The Trust tool will be finalized by M19, including integration reputation computation mechanism. In addition the final prototype for testing will require the implementation of 1) mechanisms to increase accuracy in detecting user behaviour and 2) solutions to reduce the possibility of false alarms when change in the user behaviour is detected, thus guaranteeing also security of the designed enabler. This phase will end in M19.

2.8.5.2 Lab Testing

Experiments similar to those described in Section 2.8.2 will be performed in a small scale (4/5 participants) in a controlled lab environment to test the first beta version of the Trust tool mobile application. In particular the following will be tested:

- Accuracy in detecting user behavior change and accordingly compute reputation score;
- Accuracy and resilience towards false alarm due to natural user behavior change;
- Overall security of the solution.

After beta testing a first alpha version will be provided in order to proceed with a next User Enrolment & Trial deployment phase. It is expected that this phase will last one month and end in M20.

2.8.5.3 Users Enrolment & Trial deployment

The Trust tool enabler will be integrated with other enablers and SocIoTal components in order to support the different experimentation phases. The integration with the following components is envisioned:

- Integration with the SocIoTal Authentication component to support user registration and control of Authentication functionalities;
- Integration with the SocIoTal Context Manager and in particular its communication module (Context Broker) to share alarm when malicious users are detected;
- Potentially integration (subject to component availability) with the EU IoT Lab and USEMP project tools to support the collection of feedback from users and KPIs computation;

In parallel, the different selected sets of trial users and developers will be engaged and introduced to the trials enabler, functionalities and objectives. A recruitment procedure similar to the one described in Section 2.6.6.3 will be performed. This phase will take about three months and is expected to end in M22.

2.8.5.4 Trial evaluation & Feedback Collection

Evaluation of the trial will be performed in two rounds with two target groups and evaluated by using both the collected in-app data and other feedback collected from questionnaires/surveys, ideally distributed within the application. The surveys will focus on collecting input from user experience, perceived degree privacy and other metric useful for the computation of KPIs presented in Section 2.8.4.1. Details about the experiment duration are reported in Table 1. It is envisioned that two main trial will take place involving initially citizen I the number of respectively 10 and 30 participants and only in the second phase developers, with the main target to challenge the provided implementation fro a security point of view. This phase will take place in M23-M25.

2.8.5.5 Corrective & Improvements actions

After the envisioned trials are performed, using the collected information, identified KPIs will be computed and results analysed. Other than aspects related to application usability, application stability (potential crashes, process performance time, etc), malicious user identification accuracy, implementation security and efficiency that will allow to create a more stable version of the

application to be used in large pilots with end users and potentially to solution exploited further after the SocIoTal project, other research insights are expected to be collected and extracted from the planned trials. The KPIs evaluation will result with a feedback that will require a following corrective and improvement action for possible emerged issues:

- Correction of detected bugs
- Improvement of components' usability
- Improvement of components performance/efficiency

This set of correction will be performed between M26 and M27 when the application will be finally available for larger city pilots.

This set of stages describing the trials evaluation performance will be distributed mainly along the second year of the SocIoTal project, starting officially on M16 and ending on M27, led by Task 5.2 of the project. While final implementation of the enabler will continue until the end of the Task, however the trials are expected to be finished and data analysed in M25 in order to be described into [15]. An example of the planning described above is shown in Figure below.

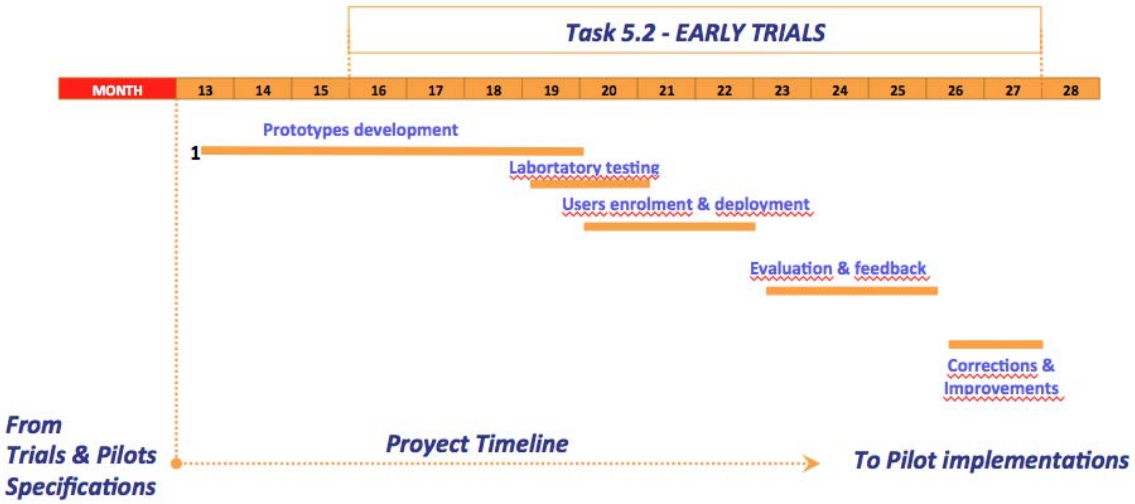

Figure 20. Timeplan for Trust tool enabler trial

2.9 Evaluating IdM and Access Control mechanisms between Bubbles (UMU)

A bubble represents a group of people and/or smart objects that communicate under the same security policies. Different types of bubbles can be defined according to the relations between people and/or smart objects. For example, a personal bubble can be composed of smart objects belonging to the same owner. Smart objects (e.g. smartphones, sensors, actuators, etc.) can maintain relationships composing different kinds of bubbles (e.g. personal or family bubble).

This trial is part of the set of evaluations carried out to verify the SocIoTal security and privacy mechanisms. Under SocIoTal foundations, each person or smart object can belong to different bubbles. In this regard, this trial evaluates the proper operation of the SocIoTal privacy preserving

Identity Management system as well the Access Control system based on capability tokens, when users want to access services or resources located out of its original or home bubble/community.

2.9.1 Scenario 5-1

Figure 21 depicts the inter bubble scenario where a smart object from a Bubble A want to access to a service located in another Bubble B. Each bubble is made up by a set of smart objects, along with an *Authorization Manager*, which is responsible for generating authorization credentials (e.g. it can be deployed on a user smartphone in the case of a personal bubble) for smart objects.

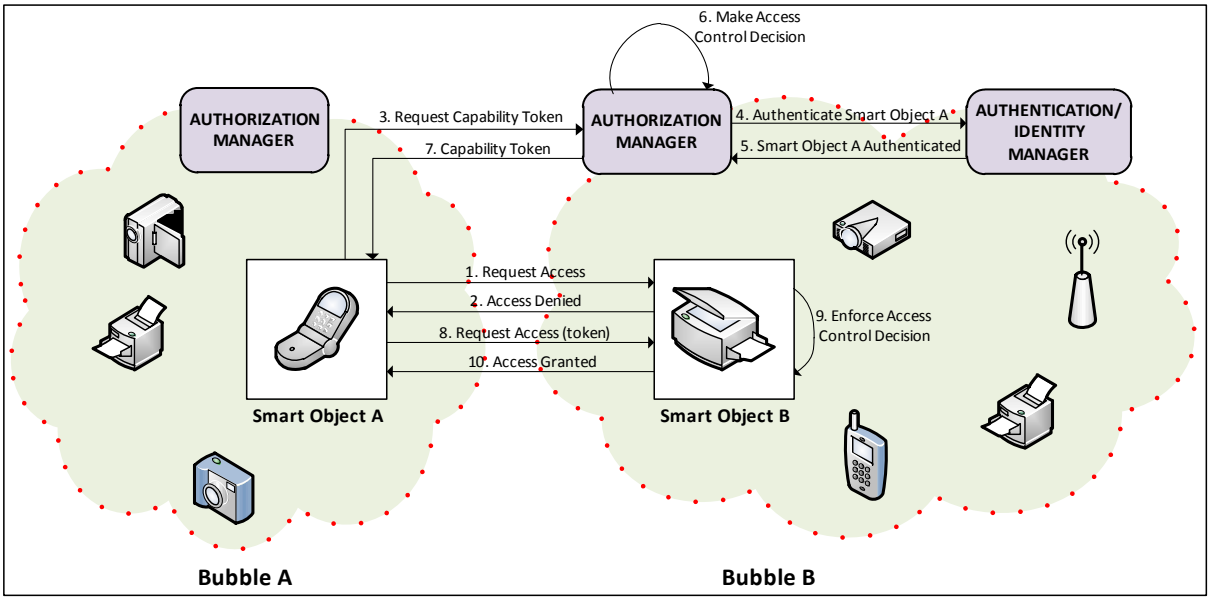

Figure 21. Access Control for SocIoTal communities and bubbles

Additionally, each bubble has an *Authentication/Identity Manager*, which is in charge of assessing the legitimacy of a smart object when it request the capability token to the Authorization Manager.

This scenario assumes a user with an android smartphone A trying to get access to a service that is provided by another android smart object B belonging to a different bubble.

2.9.2 Use case 5-1.1. Privacy preserving authentication with Partial Identities

The smartphone A performs a request to access to some service in device B. Before the authorization process is performed, device B needs to verify that the requester smart object is who it claims to be. This process is done by the IdM system, which is based on anonymous credential system defined in deliverable D2.1 [12], allowing preserving the privacy of the smartphone A. Under this approach, user A can be authenticated with their partial identities (anonymous credentials) to ensure minimal disclosure of personal and private information.

The use case assumes that the user has already configured the privacy policies which indicate which partial identity (and which particular attributes) can be used against a particular bubble in a particular context. The use case requires the smartphone of the user A to have installed the SocIoTal IdM to perform the credential presentation process. Similarly it requires the target device B to have installed the IdM to be able to verify the incoming identity credential.

It should be noticed that both, subject smartphone A and target device B trust the third entity acting as Issuer of identity credentials. This use case finalizes when the smartphone A has been successfully authenticated against device B using its partial identity, ensuring at the same time its privacy and minimal disclosure of personal information.

2.9.3 Use case 5-1.2. Inter-bubble Authorization with capability token

This use case requires a first *offline* stage where the smartphone of user A contacts with the Authorization Manager in order to get an authorization credential (i.e. a capability token) to get access to smart objects from bubble B. Notice that this phase requires the authentication of user A against the Identity Manager.

Once the smart object A is successfully authenticated, the Authorization Manager evaluates the XACML (eXtensible Access Control Markup Language) policies using the policy engine and makes an authorization decision. In case of a *Permit* decision, the PDP (Policy Decision Point) generates a capability token with the set of privileges associated to the smart object over bubble B.

After the smart object A has received the token, it makes use of it to get access to a service/resource being hosted on the smart object B. When the smart object B receives the access request, it firstly authenticates smart phone A (it can be done following the process described in the previous use case or by means of another traditional authentication mechanism). Then, device B checks whether the token is valid or not checking the signature and if the token has expired. Afterwards, as the access rights are contained in the token, the device B checks them against the requested action, including the conditions described in the token (if any). If these conditions are satisfied, the request is accepted and the service/resource is provided to the smartphone A.

2.9.3.1 List of Key Performance Indicators (KPI)

This section presents a set of tables which shows the Key Performance Indicators selected for the trial of the Privacy-preserving IdM and Access Control across Bubbles.

KPI Id:	001	KPI title:	Number of evaluators
Definition:	Number of people from the target groups that will evaluate the IdM and AC modules.		
Unit:	Number of people		
Criteria:	The greater the number of people who evaluate the trial, greater the success of the KPI.		
Relevance:	Medium relevance. It is not considered as high relevance because even if there are not many people involved in the evaluation it can be successful if the most failures and interesting improvements are discovered.		

KPI Id:	024	KPI title:	User trust
Definition:	User trust measures the grade of trust perceived by users in utilizing the application		
Unit:	Scale from 1 to 10		
Criteria:	Low levels of the scale represent low levels of trust while high levels represent a high level of trust on the experience in the use of the application.		
Relevance:	High relevance. The perceived trust is one of the strong points of the IdM and AC components.		

KPI Id:	035	KPI title:	Successful anonymous authentication
Definition:	Percentage of attempts to be authenticated and the times the user/device is successfully authenticated (having the proper credentials)		
Unit:	Boolean		

Criteria:	A high percentage will represent a high level of accuracy of the IdM in real time situation. The percentage should be close to 100%
Relevance:	High relevance to assess the correct implementation of the Identity Manager.

KPI Id:	036	KPI title:	Partial Identities
Definition:	Possibility for users to use different partial identities		
Unit:	Boolean		
Criteria:	The IdM must allow having different partial identities (i.e. credentials) with different personal attributes		
Relevance:	High relevance to assess the correct implementation of the Identity Manager.		

KPI Id:	037	KPI title:	Minimal personal disclosure
Definition:	Users can be authenticated using only the minimal set of personal attributes required by the accessed device		
Unit:	Boolean		
Criteria:	Presenting a credential holding only the requested identities attributes is enough to be authenticated.		
Relevance:	High relevance to assess the correct implementation of the Identity Manager.		

KPI Id:	038	KPI title:	Identity Credentials integrity
Definition:	The anonymous credentials cannot be forged to be used by another entity		
Unit:	Boolean		
Criteria:	The IdM provides means to sign the credentials and ensure integrity		
Relevance:	High relevance to assess the correct implementation of the Identity Manager. Unsigned or fake identity credentials cannot be used to be authenticated.		

KPI Id:	039	KPI title:	Tokens integrity
Definition:	The capability token with the access control grants cannot be falsified		
Unit:	Boolean		
Criteria:	The Access control enabler provide means to sign the tokens to ensure integrity		
Relevance:	High relevance. Unsigned or fake access control tokens cannot be used to gain access to the resource or service		

KPI Id:	040	KPI title:	Access Control Policies
Definition:	The community or bubble administrator can define access control policies in XACML to protect resources prior issuing authorization tokens.		
Unit:	Boolean		
Criteria:	Authorization XACML policies allows to describe subjects to access to target devices under certain context conditions		
Relevance:	High relevance to assess the correct implementation of the Access Control system		

2.10 Evaluating the Secure Group Sharing mechanism (UMU)

The realization of IoT scenarios with entities composing dynamic communities requires the definition of appropriate mechanisms in order to design a scalable and distributed security solution for the

envisioned use cases. Given the pervasive, dynamic and distributed nature of IoT, it is necessary to consider more flexible data-sharing models in which some information can be shared with a group of entities or a set of unknown receivers and, therefore, not addressable a priori. Indeed, unlike current Internet, in such dynamic coalitions, IoT interaction patterns are often based on short and volatile associations between entities without a previously established trust link. Providing basic security properties to such data exchange is a paramount security issue that also needs to be properly addressed.

2.10.1 Scenario 5-2

According SocIoTal foundations, the Figure 22 shows a scenario in which the Secure Group Sharing mechanism is applied. Specifically, the scenario is based on the publish/subscribe sharing model, and the use of CP-ABE (ciphertext-policy attribute-based encryption) scheme. As shown in figure, four different entities are required: a set of data producers (which publish information), a set of data consumers (showing interest on specific kinds of information), the SocIoTal broker (storing data from producers and delivering to corresponding consumers), and an Attribute Authority (in charge of generating CP-ABE keys according to a set of identity attributes).

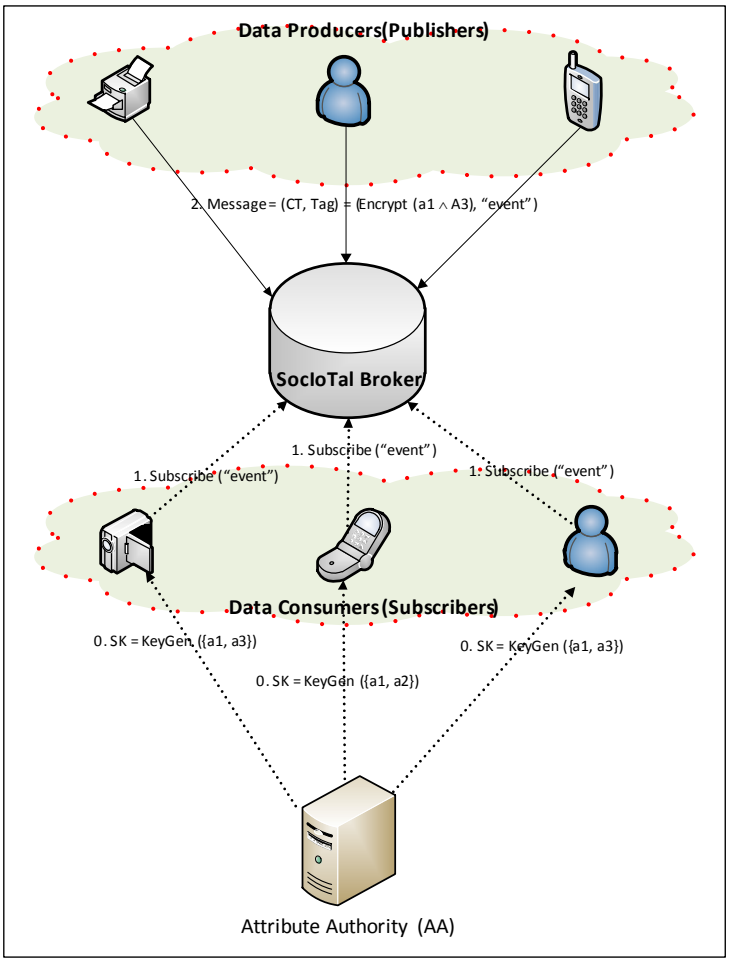

Figure 22. SocIoTal secure group sharing

2.10.2 Use case 5-2.1: Sharing keys generation

During an offline phase, data consumers get CP-ABE keys, which are associated with a set of attributes of their identity. These keys are generated by an Attribute Authority (AA) entity. The attributes associated to CP-ABE keys can be proved to the Attribute Authority through an authentication token or credential issued by a trusted entity.

2.10.3 Use case 5-2.2: Sharing policies evaluation and encryption

The secure group sharing mechanism is performed during an online phase. Firstly, when a data producer (or a set of them) decides to publish a certain data on the SocIoTal broker, it notifies its *Group Manager* component to perform this dissemination in a secure way for a set of potential consumers. The Group Manager is the component responsible for encrypting data. Furthermore, the decision on which CP-ABE policy to use for this data can be determined by different factors. Such aspects are specified in the form of *Sharing Policies*, which are evaluated in order to select the most suitable CP-ABE policy to use, according to current context, or type of data to be published. The result of this evaluation is a CP-ABE policy which is used to encrypt the data.

2.10.4 Use case 5-2.3: Data sharing through the Broker

Users share information each other through a Sociotal broker accessible by the consumers. During the offline stage, once the cryptographic keys are delivered to data consumers, they show interest in a specific event and, consequently, they subscribe themselves on the SocIoTal broker.

Then during the online stage, after the data encryption is carried out (use case 5-2.2), the resulting ciphertext is attached with a specific tag (e.g. “event”), and sent to the SocIoTal broker. Consequently, this entity can match the received tag with the interest specified previously by data consumers (i.e. subscribers). However, while this information is disseminated to the set of subscribers that showed interest on “event”, only those entities with CP-ABE keys satisfying the CP-ABE policy used to encrypt data, will be able to decrypt the information.

2.11.2. List of Key Performance Indicators (KPI)

This section presents a set of tables which shows the Key Performance Indicators selected for the trial of the Secure Group Sharing mechanism.

KPI Id:	001	KPI title:	Number of evaluators
Definition:	Number of people from the target groups that will evaluate the Group Manager component		
Unit:	Number of people		
Criteria:	The greater the number of people who evaluate the trial, greater the success of the KPI.		
Relevance:	Medium relevance. It is not considered as high relevance because even if there are not many people involved in the evaluation it can be successful if the most failures and interesting improvements are discovered.		

KPI Id:	024	KPI title:	User trust
Definition:	User trust measures the grade of trust perceived by users in utilizing the application		
Unit:	Scale from 1 to 10		
Criteria:	Low levels of the scale represent low levels of trust while high levels represent a high level of trust on the experience in the use of the application.		
Relevance:	High relevance. The perceived trust is one of the strong points of the Group Manager component		

KPI Id:	041	KPI title:	Successful subscription process
Definition:	Data consumers are able to show interest in specific information, and they are enabled to subscribe to it on the SocIoTal broker.		
Unit:	Boolean		
Criteria:	A high percentage will represent a high level of accuracy of the Group Manager in real time situation. The percentage should be close to 100%		
Relevance:	Medium relevance to assess the correct implementation of the SocIoTal broker		

KPI Id:	042	KPI title:	Successful publication process
Definition:	Data producers are able to put information on the SocIoTal broker that is tagged according to a specific label value.		
Unit:	Boolean		
Criteria:	A high percentage will represent a high level of accuracy of the Group Manager in real time situation. The percentage should be close to 100%		
Relevance:	Medium relevance to assess the correct implementation of the SocIoTal broker		

KPI Id:	043	KPI title:	Successful key generation
Definition:	Percentage of attempts to be authenticated and the times the user/device gets a key associated to the attributes that are proved during the authentication process		
Unit:	Boolean		
Criteria:	A high percentage will represent a high level of accuracy of the Group Manager in real time situation. The percentage should be close to 100%		
Relevance:	High relevance to assess the correct implementation of the Attribute Authority.		

KPI Id:	044	KPI title:	Data encryption
Definition:	The possibility for data producers to encrypt a specific information with a particular CP-ABE policy		
Unit:	Boolean		
Criteria:	The Group Manager must allow encrypting information with different CP-ABE policies specifying a combination of identity attributes values.		
Relevance:	High relevance to assess the correct implementation of the Group Manager.		

KPI Id:	045	KPI title:	Data decryption
Definition:	Only users satisfying the CP-ABE policy which is used to encrypt a specific information, will be able to decrypt the data		
Unit:	Boolean		
Criteria:	The Group		
Relevance:	High relevance to assess the correct implementation of the Group Manager.		

2.11 Evaluating the Location-aware Access Control for indoor environments (UMU)

This trial is part of the set of evaluations carried out to verify the SocIoTal security and privacy mechanisms. This trial evaluates the proper operation of the SocIoTal Capability based Access Control system along with the Indoor location enabler. The trial manages the access control between two smart objects taking into account the context coming from the Indoor location enabler explained in D3.1.

The indoor localization solution uses the smartphone built-in magnetic sensors to make security mechanisms totally independent on the type of devices and available signals in buildings. The sensed magnetic field is a combination of the effects of the Earth's magnetic field and that of surrounding objects. The effect of surrounding objects can be divided into deterministic interference, which includes the effect of ferrous materials (soft iron) and magnetized materials (hard iron), and non-deterministic interference. The effect of nearby objects can distort or even drown out the weaker direction of the Earth's magnetic field for navigation and localization purposes in buildings.

A methodological approach is used to generate the buildings maps containing the magnetic field distribution used as map of fingerprints. Then, based on such maps, location estimations are calculated using a combination of Radial Basis Functions Networks and Particles Filters.

Using the magnetic field maps of the buildings, an indoor location service is responsible for computing the position of a device inside the building. In this way, devices can ask this service in order to get the distance where a requester user is placed when trying to access to their services; consequently, certain services can be only provided when users are placed inside the authorization zone of some smart objects.

2.11.1 Scenario 5-3.1

The smartphone A acting as a subject requests to get access a resource being provided by the smart device B. Before allowing it to access to his resource, the target device B evaluates both the capability token as well as the A's position, which must be located inside B's security zone. The context that determines the smart object B position comes from the indoor localization enabler, which relies on magnetic field measurements.

Figure 23. Location-aware access control for indoor environments

2.11.2 Use case 5-3.1: Location based Access Control

Firstly, the use case requires an *offline* stage where the smartphone of user A contacts with the Authorization Manager in order to get an authorization credential (i.e. a capability token) to get access to smart objects. Notice that this phase requires the authentication process. Once the smart object A is successfully authenticated, the Authorization Manager evaluates the policies and generates (if allowed) a capability token with the set of privileges associated to the smart object.

Figure 23 depicts the main interactions of the use case. Once the smartphone has the token, a smartphone A acting as subject device wants to make use of a resource hosted by device B. The smartphone A uses its capability token to present it against device B, which validates the token

(signature, grants, etc.) and checks A's position against a localization service, since only those devices located near to B are allowed to get access.

2.11.3 Use case 5-3.2: Indoor location based on magnetic measurements

The Indoor location service analyses the magnetic field measurements coming from the device to come up with the location of the subject device. Then the location position is send back to the device B that checks the token and the position and makes an authorization decision. In order to obtain the location the Indoor location service uses the generated buildings maps containing the magnetic field distribution.

2.11.3.1 List of Key Performance Indicators (KPI)

This section presents a set of tables which shows the Key Performance Indicators selected for the trial of the location-aware access control for indoor environments.

KPI Id:	001	KPI title:	Number of evaluators
Definition:	Number of people from the target groups that will evaluate the Location-aware access control for indoor environments		
Unit:	Number of people		
Criteria:	The greater the number of people who evaluate the trial, greater the success of the KPI.		
Relevance:	Medium relevance. It is not considered as high relevance because even if there are not many people involved in the evaluation it can be successful if the most failures and interesting improvements are discovered.		

KPI Id:	024	KPI title:	User trust
Definition:	User trust measures the grade of trust perceived by users in utilizing the application		
Unit:	Scale from 1 to 10		
Criteria:	Low levels of the scale represent low levels of trust while high levels represent a high level of trust on the experience in the use of the application.		
Relevance:	High relevance. The perceived trust is one of the strong points of the Location-aware access control for indoor environments		

KPI Id:	046	KPI title:	Indoor location enabler accuracy
Definition:	Checks that the indoor location enabler provides proper location measurements inside the building. Calculated position compared to the real position.		
Unit:	Percentage		
Criteria:	A high percentage will represent a high level of accuracy of the Indoor location enabler in a real time situation.		
Relevance:	High relevance to assess the correct implementation of the Indoor location enabler.		

KPI Id:	047	KPI title:	Proper access control decisions
Definition:	Checks that only those subjects with proper and valid capability tokens can gain access to the resource		
Unit:	Percentage		
Criteria:	A high percentage will represent that the access control system validates and		

	evaluates properly the tokens and nobody can access if the token is invalid.
Relevance:	High relevance to assess the correct integration of the Indoor location enabler and the access control system.

KPI Id:	047	KPI title:	Proper access control decisions based on context
Definition:	Checks that users out of the scope of the security zone cannot gain access to the target resource.		
Unit:	Percentage		
Criteria:	A high percentage will represent that the system does not permit anybody to access the resource if it is out of the security zone.		
Relevance:	High relevance to assess the correct integration of the Indoor location enabler and the access control system.		

KPI Id:	048	KPI title:	Tokens integrity
Definition:	The capability token with the access control grants cannot be falsified		
Unit:	Boolean		
Criteria:	The Access control enabler provide means to sign the tokens to ensure integrity		
Relevance:	High relevance. Unsigned or fake access control tokens cannot be used to gain access to the resource or service		

Section 3 - Pilots (UC)

The selected SocIoTal service pilots fulfil two of the most important achievements of the project: to bring to the final users the platform, tools and the developed enablers together, including the mechanisms designed to engage and enrol them and, as a result, collect the feedback provided related to the user experience, performance and acceptance of the SocIoTal innovations. This way, a proper performance of the selected pilots will conform the best method to evaluate SocIoTal as a whole.

Section 3 will describe the services and pilots to be deployed during the last year of SocIoTal, as well as the evaluation process and the test defined for each one to evaluate its correct execution. The selected pilots come from the work done in Task 1.1, evolved through the progress in the rest of the SocIoTal WPs and refined with several meetings and co-working sessions. As the result, but still having further to go, the below specified pilots will provide scenarios to play and test all the innovations introduced by SocIoTal, as well as the selected platforms to build its running instantiation.

3.1 Pilots' Evaluation Process

Final service pilots' versions are planned to be deployed and evaluated during the last year of the SocIoTal project, led by Task 5.3 and starting on M25. Here is presented the general evaluation process envisioned for these pilots, based on the different pre-selected scenarios descriptions provided within D1.1 [16]. The initial analysis made of the work reported by Task 1.1, using feasibility, communities involved and SocIoTal enablers and features coverage criteria, produced the here described set of service pilots. Together is also extracted the general steps to evaluate each service, overall focused on the fulfilment of SocIoTal objectives and in particular, on the final users' experience.

For every set of city pilots we can define different target groups for evaluation:

- End users, i.e. citizens
- service developers (SW and HW)
- SW and HW DIY
- Policy ecology

As evaluation methodologies and tools we have considered:

- questionnaires
- qualitative interviews
- workshops
- real life testing – pilot tests

Input for the evaluation process comes from: platform architecture, mechanisms and tools to be tested by citizens, defined KPIs and involved target groups. Output from the evaluation process will allow other WPs to identify missing or improvable functionalities and improve the solutions that will be integrated in the final pilots. In addition, feedback of the end-uses will enable improvement of developed APIs (as part of WP4) and to foster engagement of the different communities to the SocIoTal concept (as part of WP6).

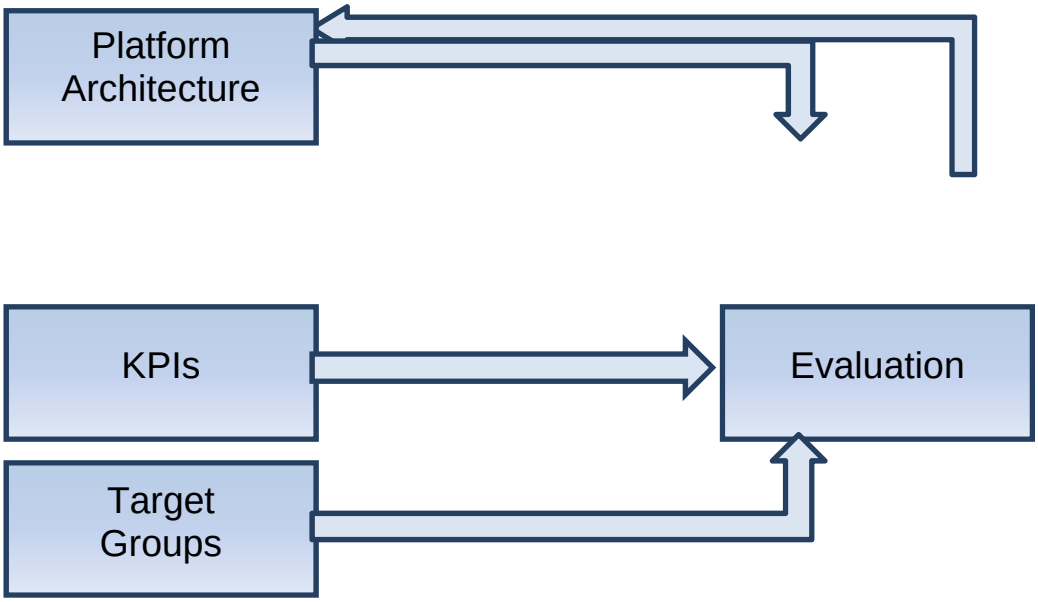

Figure 24. Evaluation process

3.1.1 Questionnaires

The questionnaires are composed with the aim to collect some useful information on improvements of the presented pilot as well as end users (i.e. citizens) satisfaction with the current implementation.

3.1.1.1 Questionnaires are to be filled at workshops by a different user groups. List of questionnaires for selection of use cases

The data is going to be collected during workshops where service is presented to the end users and their feedback collected for the further pilot improvement.

The citizens' questionnaire:

1. Do you think the application is useful for the citizens? Why?
2. What is good about the concept of this application/service?
3. What is bad about the concept of this application/service?
4. Do you think this is an interesting application for the citizens from a societal perspective?
    - no opinion
    - strongly disagree

- disagree
- neutral
- agree
- strongly agree

5. Do you think that this application might violate your privacy? Why?

6. Do you think this is an interesting application for the citizens?

    a. From an economic perspective, e.g. saves costs?
    (no opinion/strongly disagree/disagree/neutral/agree/strongly agree)

    b. From a security perspective, e.g. avoid using damaged elevator?
    (no opinion/strongly disagree/disagree/neutral/agree/strongly agree)

The developers' questionnaire:

What do you think about the concept?

- It is well conceived
- It is good but I would partially change it
- Not good. I would change it completely

If you would change something about the application what will it be?

What do you think of the design/functionalities?

- How does it look
- Are you able to do the things you want to
- How is it to navigate
- What other features would you like the app to provide

As developer do you have any general comment about this application that would increase its value in any way?

3.1.2 Pilot trials evaluation plan

Two phases are planned for the evaluation of the use cases and both will be carried out with two groups of users: developers and citizens. In Table 1 evaluation plan is provided for all pilot trials. As described in DoW total number of users involved in the pilot trials will be around 200 users for all trials that are going to be performed.

Scenario name	Users' group	Period 1	Number of initial users	Period 2	Number of initial users
Sharing Info	Developers	February (M30)	10	April (M32)	30
	Citizens	February (M30)	10	April (M32)	40
Enabling Santander (DISMAP)	Developers	November (M27)	4	February (M30)	4
	Citizens	January (M29)	15	April (M32)	40
Mood of the city	Developers	January	5	February	10
	Citizens	January	20	February	30

Elevator supervisor	Developers	January	5	February	10
	Citizens	January	20	February	30

Table 1. Pilot trials evaluation plan

3.1.3 Workshop

To be organized for different target groups. Brief introduction to project and use cases are presented. Participants are encouraged to perform some of the use cases and provide their feedback by completing the questionnaires. A main target groups are developers and citizens.

3.1.4 Collaboration with other projects

A closer collaboration with CityPulse is planned as a next step toward opening SocIoTal's platform for integration in order to engage more developers and users. As a result of this collaboration, through joint Workshops and developers' contests, both projects can benefit from the real-time evaluation of the pilots and the users' feedback.

3.2 Santander Pilots (UC)

3.2.1 Sharing information

Sharing information service will provide citizens with a platform that allows them sharing own data (from their resources) only with people to whom they give permission, within a secured and trusted environment. This pilot will use mainly the Registering users/devices, Community Creation and Discovery tools but can be easily modified to include other enablers as the Face-2-Face one or the User Trust tool. The pilot will be oriented to developers' community and people involved in Santander's IoT Meetups (together initially estimated in about 50 people) and special effort will be done with Arduino's and Raspberry–Pi communities, providing tutorials and tools to easily build SocIoTal compliant prototypes. The final pilot deployment will be opened to every user that would like to share data and/or use shared one.

3.2.1.1 Operational description

Users will firstly register themselves against the platform through the SocIoTal Registering Tool [1]. The interface will ask the user a minimum set of data such as their name, their ID number, etc. That information will be modelled by the tool following the SocIoTal Data Modelling format and sent to the platform in charge of gathering all the Identity registrations. Once the information has been checked and stored, the core platform will register the user and will return their identification and security information needed to realise future actions.

Once the user is registered they will be able to register their devices. All devices capable to send their measurements (generate context) to a server are susceptible to be registered within the SocIoTal platform. Users can share different kind of information from different sources, for example, citizens can share information gathered by the sensors included within their smartphones or tablets. In the case that they are more interested in technological DIY gadgets they could build their own devices such as weather stations through Arduino or Raspberry Pi boards and different sensors (temperature, humidity, pressure, etc.) and in an easy way program them to send their observations to the recipient platform. For this purpose, SocIoTal will perform some workshops in order to teach citizens, interested in this process, how to build their own weather stations (extensible to other kind of monitoring depending of the sensors used). Apart from information gathered by their IoT devices, users will be able to share different information such as documents in a secure way making use of the security framework offered by the SocIoTal platform.

The strong point of the pilot is the functionality of sharing the information and context data provided by users among the users, and this is formalized through the Community Creation enabler. Users will be able to create and manage a community, i.e. a group where they can share information among members within a security framework. The owner of the community (the person who creates the community), through the SocIoTal Community Creation tool [2], fills the information needed to create the community such as info about the owner, access policies, members, devices to share, etc. Once they have filled the information it is formatted according the SocIoTal Data Modelling and pushed to the platform.

Once the Community has been created, a member will be able to access information produced by the rest of members in the community through the User Interface. To request information about users, devices or observations within the community the users will complete the needed information to describe what are they looking for, and the SocIoTal Discovery tool [1] will be in charge of discover all data related to the request that users are allowed to access.

In addition to this, citizens may be interested in receiving information following a pub/sub pattern. They would subscribe their profile to some devices/observations and they would receive notifications when a new value is sent from the device, an observation is updated or when a "when something do something" paradigm established by the user occurs. Also, to enrich the overall scenario, F2F enabler [14] can be used to identify a user or device and start the sharing or discovering services process.

3.2.1.2 Test cases

Test Id:	001	Test title:	Usability
Test Objective: This test aims to measure the usability of the Registration, Discovery and Community Creation tools, working together, from the point of view of the final user, through the user interface.			
Pre-requisites: The user will have to access the tools from a device that supports the last release of the application.			
Test Environment: Users accesses the user interface and register users/devices, create communities and discovery other users/devices/observations.			
Evaluation Method: Users from different target groups will be approached from workshops, local newspaper, etc. After some time using the application, all of them will be asked to fill a questionnaire where different aspect about the usability will be remarked. Also, a smaller group from workshops will be personally interviewed to discover how they interact with the tool, this way we will can find what are the reactions and the how easy-to use is the environment for the user. Besides, an email communication channel will be created in order to receive feedback from the users.			
Metric(s): Scale from 0 to 10.			
Expected Result: From a statistical study a result about an average of 8 is expected.			
Remarks: Apart from the statistical results extracted from the scale values, there will be studied also different textual opinions provided as comments during the questionnaires or interviews.			
Test result: Statistical results will be presented graphically and comments will be presented as a list of more relevant suggestions and beliefs about usability.			

Test Id:	002	Test title:	People registration
Test Objective: This test will measure the percentage of people registration failures and the registration performance times.			
Pre-requisites: The user will have to access the tool from a device that supports the last release of the tool and facilitate the minimum data required for the registration.			
Test Environment: Users access the tool and register themselves within the SocIoTal platform.			
Evaluation Method: Users from different target groups will be approached from workshops, local newspaper, etc. After some time using the application, all of them will be asked to fill a questionnaire			

where aspects about the registering will be asked. Also, a smaller group from workshops will be personally interviewed to discover how they interact with the tool, and how many problems they face when they to register themselves within the platform. Besides, an email communication channel will be created in order to receive information about possible problems during the process and feedback from users. Performance explicit times would be collected from SocIoTal platform logs.
Metric(s): Percentage of failures. Time (seconds) expended to perform a user registration.
Expected Result: It will be studied the number of failed records divided among all registration attempts (extracted by statistical studies). It is expected an average of no more than 10% of failures.
Remarks: In addition to the statistical results a list of different opinions and suggestion from users in order to improve the way they register themselves within the platform will be presented.
Test result: statistical results will be presented graphically and comments will be presented as a list of more relevant suggestions and comments about the registering tool.

Test Id:	003	Test title:	Device registration
Test Objective: This test will measure the percentage of device registration failures and the registration performance times.			
Pre-requisites: The user will have to access the tool from a device that supports the last release of the tool. Also, users will facilitate the minimum data required for the registration.			
Test Environment: Users register their devices through the application (User Interface).			
Evaluation Method: Users from different target groups will be approached from workshops, local newspaper, etc. After some time using the application, all of them will be asked to fill a questionnaire where aspects about the device registering will be asked. Also, a smaller group from workshops will be personally interviewed to discover how they interact with the tool, and how many problems they face when they try to register their devices within the platform. Besides, an email communication channel will be created in order to receive information about possible problems during the process and feedback from users. Performance explicit times would be collected from SocIoTal platform logs.			
Metric(s): Percentage. Time (seconds) expended to perform a user registration.			
Expected Result: It will be studied the number of failed records divided among all registration attempts (extracted by statistical studies). A result about an average of no more than 10% of failures is expected.			
Remarks: In addition to the statistical results it will be offered different opinions and suggestion from users in order to improve the way the devices are registered within the platform.			
Test result: statistical results will be presented graphically and comments will be presented as a list of more relevant suggestions and beliefs about the registering tool.			

Test Id:	004	Test title:	Community Management
Test Objective: this test aims to calculate the failures detected when a user tries to: • Create a community • Update community Info • Delete community • Register within an existing community It will also include the different performance times.			
Pre-requisites: The user will have to access the tool from a device that supports the last release and will facilitate the minimum data required for the community management.			
Test Environment: Users access the Community Management tool and create a new community			

through the user interface. They will also be able to update the selected community info and register/unregister within a given community.
Evaluation Method: Users from different target groups will be approached from workshops, local newspaper, etc. After some time using the application, all of them will be asked to fill a questionnaire where aspects about the community creation will be asked. Also, a smaller group from workshops will be personally interviewed to discover how they interact with the tool, and how many problems they face when they manage a community through the tools provided. Besides, an email communication channel will be created in order to receive information about possible problems during the process and feedback from users.
Metric(s): Percentage. Time (seconds) expended to perform different community management processes.
Expected Result: It will be studied the number of failed Community Management processes divided among all attempts (extracted by statistical studies). It is expected a result about an average of no more than 10-15% of failures.
Remarks: In addition to the statistical results it will be offered different opinions and suggestion from users in order to improve the way communities are managed within the platform.
Test result: statistical results will be presented graphically and comments will be presented as a list of more relevant suggestions and beliefs about the community creation tool.

Test Id:	005	Test title:	Entities discovery (People, Resources, Observations/Datatypes)
Test Objective: this test will measure the percentage of failures when a user attempt to discover an entity (context entity) using the provided platform. A context entity here could be a registered user (person) or a smart object (device, resource, information source…). Although are not considered as "entities", the observations or data types provided by the context entities could also drive the discovering process (e.g. discover all entities that provide temperature observations within this selected area). Execution times of the discovery processes will be also captured.			
Pre-requisites: The user will have to access the tool from a device that supports the last release. Also, users will have to facilitate the minimum data required for the discovery.			
Test Environment: Users access the Discovery tool and look for other entity and/or info available according their profile through the user interface.			
Evaluation Method: Users from different target groups will be approached from workshops, local newspaper, etc. After some time using the application, all of them will be asked to fill a questionnaire where aspects about the people discovery will be asked. Also, a smaller group from workshops will be personally interviewed to discover how they interact with the tool, and how many problems they face when they search for other users, entities or datasets within the platform. Besides an email communication channel will be created in order to receive information about possible failures and feedback from users. Three mainly different cases will be considered as failures during the test: • User does not find other entities that should be found • Users find entities that they are not allowed to find • Application crashes			
Metric(s): Percentage. Time (seconds) expended to perform different discovering processes.			
Expected Result: It will be studied the number of failed entities discovery processes divided among all process attempts (extracted by statistical studies). A result about an average of no more than 20% of failures is expected.			
Remarks: In addition to the statistical results it will be offered different opinions and suggestion from users in order to improve the way they discover other users within the platform.			

Test result: statistical results will be presented graphically and comments will be presented as a list of more relevant suggestions and beliefs about the discovery tool.

Test Id:	006	Test title:	Subscription to alerts
Test Objective: This test aims to measure the failure rate of subscription processes.			
Pre-requisites: The user will have to access the service from a device that supports the last release of the application and facilitate the minimum data required for the subscription.			
Test Environment: Users will create alert subscriptions in order to receive in the future alerts and notifications about concrete observations or devices.			
Evaluation Method: Users from different target groups will be approached from workshops, newspapers, etc. After some time using the application, all of them will be asked to fill a questionnaire where aspects about subscription process will be asked. Also, a smaller group from workshops will be personally interviewed to discover how they interact with the tool, and how many problems they face when they create a subscription to an alert within the platform. Besides an email communication channel will be created in order to receive information about possible failures and feedback from users.			
Metric(s): Percentage			
Expected Result: It will be studied the number of failed alert subscriptions processes divided among all subscription creation process attempts (extracted by statistical studies). A result about an average of no more than 10% of failures is expected.			
Remarks: In addition to the statistical results it will be offered different opinions and suggestion from users in order to improve the way the subscription to alerts is performed.			
Test result: statistical results will be presented graphically and comments will be presented as a list of more relevant suggestions and beliefs about the subscription service.			

Test Id:	007	Test title:	Alert reception
Test Objective: This test aims to measure the alert reception failures.			
Pre-requisites: The user will have to access the tool from a device that supports the last release.			
Test Environment: Users will receive alerts and notifications related to the subscription they have created.			
Evaluation Method: Users from different target groups will be approached workshops, newspapers, etc. After some time using the application, all of them will be asked to fill a questionnaire where aspects about alert reception will be asked. An email communication channel will be created in order to receive information about possible failures and feedback from users.			
Metric(s): Percentage			
Expected Result: It will be studied the number of failed alert reception divided among all subscription alerts that should be received (extracted by statistical studies). It is expected a result about an average of no more than 10% of failures.			
Remarks: In addition to the statistical results it will be offered different opinions and suggestion from users in order to improve the way the subscription to alerts is performed.			
Test result: statistical results will be presented graphically and comments will be presented as a list of more relevant suggestions and beliefs about the subscription service.			

3.2.2 Enabling Santander –DISMAP

DISMAP (Accessible routes for Disabled People Navigator) is an initiative led by an external group of developers (from the city of Santander) to be built over the platform (tools and enablers) provided by SocIoTal project. It was captured as a result of the Santander City Brain [17], as the "most innovative

business project for Santander City award" winner, and, through the first Santander IoT Meetup, it was incorporated to SocIoTal as one of its scenarios. DISMAP will provide disabled citizens with an application to go from one place to another in the city, avoiding barriers along their journey (works, road closed, narrow sidewalk, etc.). It will create a community of users (oriented to disabled people but open to every user that can benefit from shared data and/or provide suitable information) and design the interfaces to upload events for routes calculation and information to be shared with other members. The DISMAP pilot has an already engaged potential community (thanks to Santander City Council and DISMAP head people) that covers the disabled people from Santander and surroundings, as well as their caregivers' communities.

3.2.2.1 Operational description

The application will make use of the SocIoTal Registration enabler [1] to complete the first step that users will follow just after they download the application: their registration. In order to complete this phase, users will fill a form with basic information that register themselves within the SocIoTal platform and give them the authorization to access to the platform and use the services. This information will help the application to provide better services to the user, for example, if the citizen uses a wheelchair the routes may be different than if the person is using crutches (maybe the sidewalk is too narrow for a wheelchair but not for a person with crutches). Also, the information showed could be different if you are a disabled person, a carer or other citizen that want to report barriers in the city like a baby's pram driver.

As it has been said, there are three main different target groups:

- Disabled citizens: people who are interested in finding routes from one point to another in the city where there are not barriers that could impede a continuous journey. Apart from search routes, they will also upload events of different nature such as notifications about barriers, notifications about interesting events for the community, etc.
- Carers citizens: this target group in direct contact with disable people is formed by family, friends and carer workers that are interested in searching routes to help disabled people to access different places in the city and facilitate their attendance.
- Other citizens: people interested in finding routes without barriers as parents with prams or deliverers. Also people interested in reporting notifications about barriers within the city to help the application to be as much complete and accurate as possible.

In order to upload events (such as an alert about a narrow sidewalk) users will have to register their devices (smartphone, tablet, etc.) within the platform. For that purpose they will fill the correspondent form and, after that, it will be automatically pushed to the platform.

It can be highlighted the application of the community concept. Thus, users will be able to create a community, through the Community Creation enabler [2], as a group of users who lives in the same area, and exchange information among them safely without leaking of information.

Within the application, the service of route calculation will make use of the SocIoTal Discovery Enabler [1]. When the user fills the form to request a route, the algorithm will need data about the places that have barriers that can involve a problem for a disabled person. That data will be requested through the Discovery Enabler tool and used to create the best route. Also, a user through the application could request data about the accessibility of a concrete area without only mark the area they want to analyse (centre and diameter, different point to make a polygon, etc.). In addition to this, if the user is interested in receiving alerts from certain events, they could create a subscription and receive alerts when the event focus of the subscription undergoes a change.

Apart from search events and observations, users may want to search other users, for example to invite them join a community.

3.2.2.2 Test cases

Test Id:	001	Test title:	SocIoTal API Usability
Test Objective: This test aims to measure the usability of the Registration, Discovery and Community Creation tools final versions, integrated with the SocIoTal Security Framework and with the rest of the enablers that will provide trusted and reliable information sharing. Usability here, from the point of view of the DISMAP developer, measures the grade of simplicity, adaptability and functionality perceived by users when they perform the corresponding tests through the SocIoTal API.			
Pre-requisites: The developer will need a development environment (an IDE like eclipse or netbeans) suitable to integrate REST services to interact with the SocIoTal provided API.			
Test Environment: The developer access the tools' APIs to perform users/devices registration, create communities, upload context information and discover other users/devices/attributes related to Disabled environment within Santander city.			
Evaluation Method: Developers will be introduced to the tools APIs and how to operate with it. After some time using the API, all of them will be asked to fill a questionnaire where aspects about the usability and services performing will be asked.			
Metric(s): Scale from 0 to 10.			
Expected Result: From a statistical study a result about an average of 8 is expected.			
Remarks: Apart from the statistical results extracted from the scale values, there will be studied also different textual opinions provided as comments during the questionnaires or interviews.			
Test result: Statistical results will be presented graphically and comments will be presented as a list of more relevant suggestions and comments about usability. Bugs and malfunctions detection. Improvements detected by developers to be integrated in further versions of the API.			

Test Id:	002	Test title:	SocIoTal API Performance
Test Objective: This test will measure the percentage of failures and the different execution times when performing users/devices registration, communities' management, context information uploads and discovering procedures using the provided SocIoTal developers API.			
Pre-requisites: The user will have to access the provided API from a device that supports the last release. Users must have a suitable IDE (Integrated Development Environment).			
Test Environment: Users (DISMAP Developers) will integrate the provided SocIoTal API within their corresponding IDE to build the functionalities required by DISMAP application.			
Evaluation Method: DISMAP developers will be trained in the use of the SocIoTal needed APIs in order to build DISMAP features over SocIoTal platform. During this DISMAP development process, UC team will trace the different SocIoTal processes performance involved, in order to capture (mainly) the failure rates and the execution times. Different processes involved here will be: • People discovery (other DISMAP community members searching) • Event (user data) creation and upload into the SocIoTal platform • Events discovery and access • Subscription to events			
Metric(s): Percentage of failures. Time (milliseconds) expended to perform different SocIoTal processes.			
Expected Result: It will be studied the number of failed records divided among all registration attempts (extracted by statistical studies). It is expected an average of no more than 2% of failures.			

Remarks: In addition to the statistical results it will be presented a list of different opinions and suggestion from users in order to improve the way they make use of the SocIoTal APIs features.
Test result: statistical results will be presented graphically and comments will be presented as a list of more relevant suggestions and beliefs about the registering tool.

Test Id:	003	Test title:	Route Quality (final result of the APP)
Test Objective: This test will measure the accuracy of the route requested by the user. A route will be considered as high quality if it takes into account all blocking elements registered in the journey and reports all needed information about them.			
Pre-requisites: User will have to access the application from a device that supports the last release of the application.			
Test Environment: Users (DISMAP community members) receive the route requested, according the info provided by the user and the context information captured by the app. The user will be able to follow this provided route from the application installed on their device.			
Evaluation Method: Users from different target groups will be approached from associations for disabled people, workshops, newspapers, etc. After some time using the application, all of them will be asked to fill a questionnaire where aspects about route quality will be asked. An email will be shared to receive bugs that users could find during the use of the application. Although this test case is not a properly SocIoTal's one (it reports DISMAP app evaluation), as DISMAP is a SocIoTal based app, it will be useful when evaluating SocIoTal features performance as a whole.			
Metric(s): It will be studied the percentage of routes resolved with high quality in comparison with the percentage of routes that does not provide accurate information about the journey.			
Expected Result: It is expected results about an 80% of routes graded as high quality routes.			
Remarks: In addition to the statistical results it will be offered different opinions and suggestion from users in order to improve the route quality.			
Test result: statistical results will be presented graphically.			

3.3 Novi Sad Pilots (DNET)

Novi Sad pilot will implement two different pilot trials: Elevator Supervisor and Mood of the city. Elevator supervisor filed trial is depicted in co-creation workshop with citizens held in Novi Sad, as one of the use cases that participants were showing the most interest for, mainly due to following reasons:

- New law requires certification, but there are only three institutions that are able to do this. Remote management would be a huge time gain as now the permits take very long and the elevator cannot function without the certificate
- Every elevator has its own closed software system. There is no back up of its history, only a maintenance book that could be anywhere in the building and is a single copy that could get lost
- Quality control could be ensured by monitoring and giving insight into the elevator utilization [18]

Mood of the city is novel concept calculated using a set of scalable inputs collected from the citizens, i.e. citizens' mood and environmental data collected from sensors.

3.3.1 Elevator Supervisor

This field trial is deployed in a resident building where sensor and application provide elevator malfunction detection, data access control and notification for multiple users as well as history track

and information about previous repairs and inspections. The main goal of the application is to enable history track of previous repairs and to signalize when the elevator maintenance should be done after certain travelled distance. The pilot is deployed using Raspberry Pie [9] board with GPRS interface, 3-axis accelerometer (Figure 25) to detect elevator movements and PIR (Passive Infrared) sensor for presence detection (Figure 26). Movements' value are logged at the SD card and evaluated in a real-time in order to detect certain behaviour.

Data is saved to a web portal which limits access to authorized users only. Data access control and notifications for multiple users (e.g. tenants, company responsible for repair, etc.) enables history track, information about previous repairs and scheduling of future repairs.

Figure 25. ADXL345 accelerometer

Raspberry Pi is used with accelerometer board Accell Click ADXL345 which supports both I2C (Inter-Integrated Circuit) and SPI (Serial Peripheral Interface) bus connection.

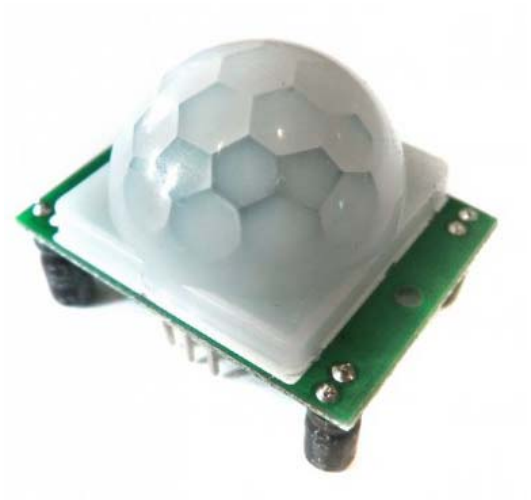

Figure 26. PIR sensor

Measuring travelled distance

Values from the z-axis which represents vertical movements of the sensor positioned horizontal on the ground are recorded in 1 second window and processed using low pass filter. After filtering signal, peaks can be analysed in order to conclude when the elevator is moving (Figure 27).

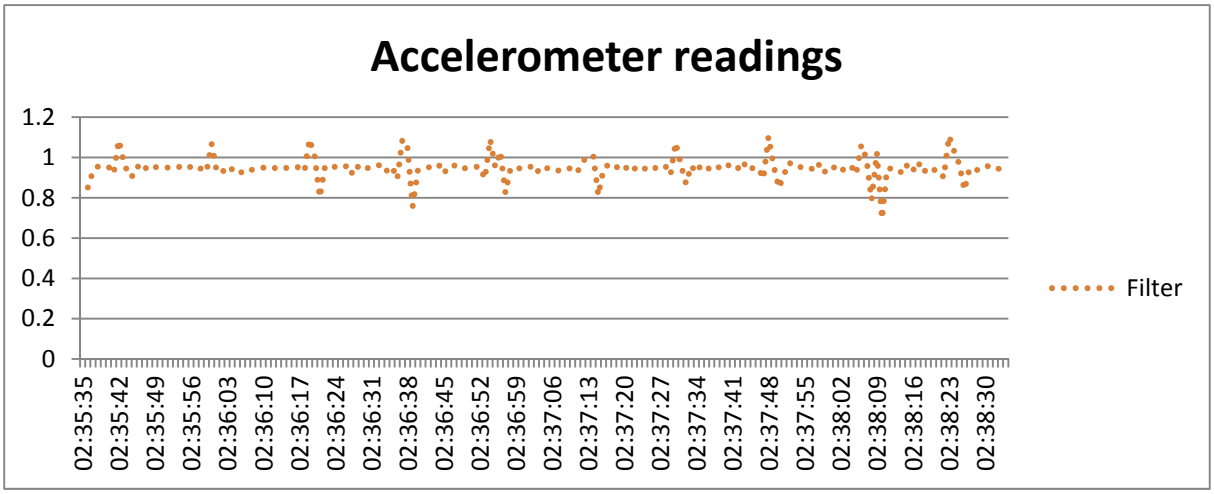

Figure 27. Accelerometer data processed with low pass filter

List of proposed pilot test cases to be prepared in order to evaluate:

- Usability
- Performance
- Robustness
- Flexibility
- Usability
- Security

3.3.1.1 Test case 1

Test Id:	001	Test title:	Usability
Test Objective: This test aims to measure the usability of the tool from the point of view of the final user.			
Pre-requisites: The user will have to access the web portal			
Test Environment: User access the web portal and start to discovery and use different functionalities offered by the tool.			
Evaluation Method: A main user group here are tenants, which will gain access to the web portal. After some time using the portal, all of them will be asked to fill a questionnaire where different aspect about the usability will be remarked. Also, a smaller group of tenants will be personally interviewed to discover how they interact with the tool, this way we will can find what are the reactions and the how easy-to use is the environment for the user.			
Metric(s): Scale from 0 to 10.			
Expected Result: From a statistical study we expect a result that provides an average of 8			

Remarks: Apart from the statistical results extracted from the scale values, there will be studied also different textual opinions provided as comments during the questionnaires or interviews.
Test result: Statistical results will be presented graphically and comments will be presented as a list of more relevant suggestions and beliefs about usability.

Test Id:	002	Test title:	Travelled distance calculation
Test Objective: This test will measure the accuracy of travelled distance calculation for the elevator			
Pre-requisites: The user will have to access the web portal			
Test Environment: User access the web portal and uses the elevator			
Evaluation Method: User will use the elevator and compare the elevator travelled distance with distance showed by the web portal.			
Metric(s): Percentage of error.			
Expected Result: The error rate is expected to be below 5%			
Remarks: In addition to the results, corrective measures will be proposed to improve results			
Test result: statistical results will be presented graphically with corrective measure proposal			

Test Id:	003	Test title:	Malfunction detection
Test Objective: This test evaluate malfunction detection accuracy			
Pre-requisites: The user will have to access the web portal and access to email.			
Test Environment: User access the web portal and email account and uses the elevator			
Evaluation Method: User will check if there is a problem with elevator functioning, and compare the report of malfunctioning with real status of elevator			
Metric(s): Percentage of error.			
Expected Result: The error rate is expected to be below 1%			
Remarks: In addition to the statistical results it will be offered different opinions and suggestion from users in order to improve the way the malfunction detection is performed.			
Test result: statistical results will be presented graphically and comments will be presented as a list of more relevant suggestions and beliefs about the malfunction detection service.			

Test Id:	004	Test title:	Only registered user access

Test Objective: This test will measure the percentage of wrong accesses to data within the platform such as not allowed accesses to data (only registered users should be able to see data). Registered users should be tenants and company responsible for repair
Pre-requisites: The user will have to access the web portal
Test Environment: User access the web portal and uses the elevator
Evaluation Method: After some time using the application, tenants and company responsible for repair will be asked to fill a questionnaire where aspects about proper accesses will be asked. Also, a smaller group will be personally interviewed to discover how they interact with the application, and how many problems they face when they access data within the platform. Also, an email will be shared to receive bugs that users could find during the use of the application. It will be studied two main issues: • Access to forbidden data • Denial of access to allowed data
Metric(s): Percentage
Expected Result: measurements of percentage of denial of access to allowed information. It is expected a result about an average of no more than 2% of security errors.
Remarks: In addition to the statistical results it will be offered different opinions and suggestion from users in order to fix security issues that could appear.
Test result: statistical results will be presented graphically

Test Id:	005	Test title:	Notifications
Test Objective: This test aims to measure the notifications reception failures.			
Pre-requisites: The user will have to access the web portal and email account			
Test Environment: User access the web portal, email. Users will receive notifications and notifications related to the subscription they have created.			
Evaluation Method: After some time using the application, tenants and company responsible will be asked to fill a questionnaire where aspects about the notifications reception will be asked. Also, an email will be shared to receive bugs that users could find during the use of the application.			
Metric(s): Percentage			
Expected Result: It will be studied the number of failed notification reception divided among all notifications that should be received (extracted by statistical studies). It is expected a result about an average of no more than 2% of failures.			
Remarks: In addition to the statistical results it will be offered different opinions and suggestion from users in order to improve the way the subscription to notification is performed.			
Test result: statistical results will be presented graphically and comments will be presented as a list of more relevant suggestions and beliefs about the notification service.			

Test Id:	006	Test title:	Look and feel

Test Objective: This test aims to measure the look and feel perceived by the user.
Pre-requisites: The user will have to access the tool from a device that supports the last release of the tool
Test Environment: User access the web portal and uses the elevator
Evaluation Method: After some time using the application, tenants and company responsible will be asked to fill a questionnaire where aspects about the look and feel will be asked. Also, a smaller group will be personally interviewed to discover how they interact with the application. Also, an email will be shared to receive bugs that users could find during the use of the application. There will be evaluated different aspects influenced by the interaction with the application such as the graphic effects, menu, buttons, colours, typography, etc.
Metric(s): Scale from 0-10
Expected Result: From a statistical study a result about an average of 8 is expected.
Remarks: Apart from the statistical results extracted from the scale values, there will be studied also different textual opinions provided as comments during the questionnaires or interviews.
Test result: Statistical results will be presented graphically and comments will be presented as a list of more relevant suggestions and beliefs about look and feel

3.3.2 Mood of the city

This pilot will enable computation of a Mood of the city defined herein as a scaled metric, derived from contextually different entities that influence people happiness and mood. Final Mood of the city value is computed using aggregated users' data, i.e. users' mood detected from an image, answers to a subjective happiness questionnaire [19], users' selections from a predefined mood list and environmental data.

Subjective happiness questionnaire is a 4-item Subjective Happiness Scale (SHS) of global subjective happiness. Two items ask respondents to characterize themselves using both absolute ratings and ratings relative to peers, whereas the other two items offer brief descriptions of happy and unhappy individuals and ask respondents the extent to which each characterization describes them.

It is worth noting that responses to the happiness measure cannot be attributed to respondents' current mood [19]. In addition, as final value will depend of a number of users posted their data, we have included well-known parameters that are proven to influence peoples' mood: environmental parameters, i.e. temperature and humidity [6].

These 3 factors together are used to build the final mood of the city index where mood of the citizens sent from devices have maximum impact factor of 50%, temperature 25% and pressure 25% on the final score.

Figure 28. Visualization of the Mood of the city

Emotion recognition from image

Before detecting emotions using camera, face region is extracted from the image. From the face mouth area is cropped and then classified using Fisherface algorithm [20] trained on a Yale dataset [21] increased with a series of custom labelled images. The algorithm is capable of detecting three types of emotions: happy, sad and normal.

Implementation is done using OpenCV android library [22].

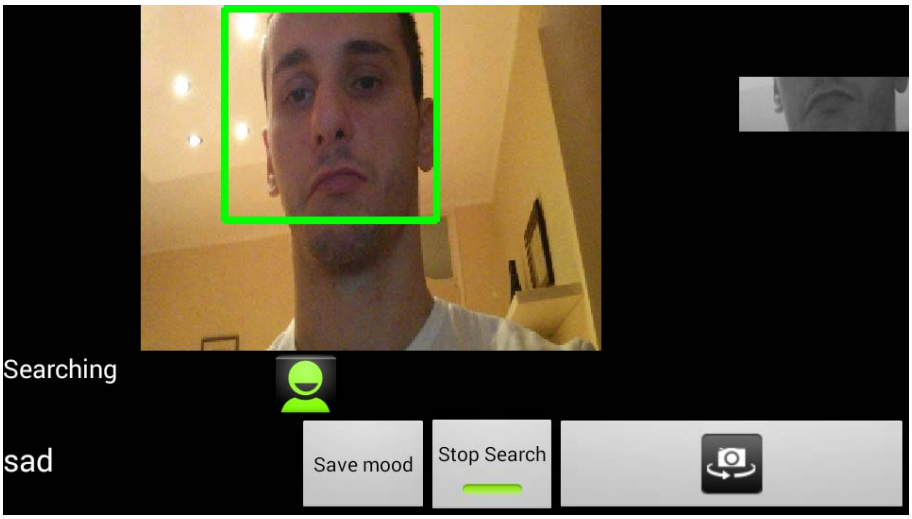

Figure 29. Detecting users' mood from device's camera

Environmental data

Temperature and humidity are summoned from ekoBUS700++ [7] devices, a sensors attached to a moving public transportation vehicles. Every two hours data is collected from these devices and saved to a local database.

List of proposed pilot test cases to be prepared in order to evaluate:

- Platform functions/services
- Performance
- Robustness
- Flexibility
- Usability
- Security

3.3.2.1 Test case 1

Test Id:	001	Test title:	Usability
Test Objective: This test aims to measure the usability of the tool from the point of view of the final user.			
Pre-requisites: The user will have to access the tool from a device that supports the last release of the tool			
Test Environment: User access the tool (via web, download the application, etc) and start to discovery and use different functionalities offered by the tool.			
Evaluation Method: Users from different target groups will be approached from workshops, meetups, etc. After some time using the application, all of them will be asked to fill a questionnaire where different aspect about the usability will be remarked. Also, a smaller group from workshops will be personally interviewed to discover how they interact with the tool, this way we will can find what are the reactions and the how easy-to use is the environment for the user.			
Metric(s): Scale from 0 to 10.			
Expected Result: From a statistical study we expect a result that provides an average of 8			
Remarks: Apart from the statistical results extracted from the scale values, there will be studied also different textual opinions provided as comments during the questionnaires or interviews.			
Test result: Statistical results will be presented graphically and comments will be presented as a list of more relevant suggestions and beliefs about usability.			
Test Id:	002	Test title:	Facial expression detection accuracy
Test Objective: This test evaluate facial expression detection accuracy			
Pre-requisites: The user will have to access the tool from a device that supports the last release of the tool			

Test Environment: User access the tool, and application is recognizing users' mood from the captured picture and other parameters from the questionnaire and environmental parameters
Evaluation Method: After determination of user mood, user will be asked to confirm if obtained mood corresponds with real mood. If real and determinate mood were different, it will be counted as an error. Measured value will be ratio between number of wrong mood estimations and total number of recognition.
Metric(s): Percentage of failures.
Expected Result: The error rate is expected to be below 10%
Remarks: In addition to the statistical results it will be offered different opinions and suggestion from users in order to improve the way the facial expression detection is performed.
Test result: statistical results will be presented graphically and comments will be presented as a list of more relevant suggestions and beliefs about facial expression detection service.

Test Id:	003	Test title:	Temperature accuracy
Test Objective: Temperature data will be compared to public available measures			
Pre-requisites: Tool collects temperature measurements from ekoBUS700++			
Test Environment: User access the tool, and application is recognizing users' mood from the captured picture and other parameters from the questionnaire and environmental parameters			
Evaluation Method: Obtained temperature measurements will be compared with public available measurements. The relative error will be defined as the measure how much percentage is the difference between measured and public values. Error rate is the ratio between the number of relative errors higher than predefined value, divided with total number of measurements.			
Metric(s): Percentage of failures.			
Expected Result: The error rate is expected to be below 5% around the public available measures			
Remarks: Apart from the statistical results extracted from the scale values, there will be studied also different textual opinions provided as comments during the questionnaires or interviews.			
Test result: Statistical results will be presented graphically and comments will be presented as a list of more relevant suggestions and beliefs about look and feel			

Test Id:	004	Test title:	Relative humidity data accuracy
Test Objective: Relative humidity data will be compared to public available measures			
Pre-requisites: Tool collects relative humidity measurements from ekoBUS700++			

Test Environment: User access the tool, and application is recognizing users' mood from the captured picture and other parameters from the questionnaire and environmental parameters
Evaluation Method: Obtained relative humidity measurements will be compared with public available measurements. The relative error will be defined as the measure how much percentage is the difference between measured and public values. Error rate is the ratio between the number of relative errors higher than predefined value, divided with total number of measurements
Metric(s): Percentage of failures.
Expected Result: The error rate is expected to be below 5% around the public available measures
Remarks: Apart from the statistical results extracted from the scale values, there will be studied also different textual opinions provided as comments during the questionnaires or interviews.
Test result: Statistical results will be presented graphically and comments will be presented as a list of more relevant suggestions and beliefs about look and feel

Test Id:	005	Test title:	Look and feel
Test Objective: This test aims to measure the look and feel perceived by the user.			
Pre-requisites: The user will have to access the tool from a device that supports the last release of the tool			
Test Environment: User downloads the application and use the different services provided by the application.			
Evaluation Method: Evaluation Method: After some time using the application, users will be asked to fill a questionnaire where aspects about the look and feel will be asked. Also, a smaller group will be personally interviewed to discover how they interact with the application. Also, an email will be shared to receive bugs that users could find during the use of the application. There will be evaluated different aspects influenced by the interaction with the application such as the graphic effects, menu, buttons, colours, typography, etc.			
Metric(s): Scale from 0-10			
Expected Result: From a statistical study a result about an average of 8 is expected.			
Remarks: Apart from the statistical results extracted from the scale values, there will be studied also different textual opinions provided as comments during the questionnaires or interviews.			
Test result: Statistical results will be presented graphically and comments will be presented as a list of more relevant suggestions and beliefs about look and feel			

Section 4 - Conclusions (DNET)

The main goal of WP5 is to design, deploy and coordinate two pilot services, so as to assess the feasibility and applicability of the techniques, procedures and functions developed during the project lifetime. The objective would be to test the developments coming from other WPs over real environments, with real users, facing all the constraints and limitations that a complex society can pose in these kinds of trials. Based on the architecture provided by WP1 and the various techniques, procedures, and protocols provided by the rest of the WPs, the trials to be used during the experimental evaluation are specified.

In this document are described the scenarios selected for the field trials and pilot deployment, together with the evaluation methodology, including relevant KPIs; those will be based on the use cases provided by WP1.

In the section 2 selected field trials are explained in details. At the beginning of the section trial evaluation process is described. Different target groups are specified (end users, SW and HW DIY and Service developers) and the ways of interaction with these groups, and the expectations in terms of evaluation. The enablers to be developed during the project life will be evaluated in different phases and within each step a target group (or several) will be approached. For each trial are presented the scenario and the use cases extracted from it in addition to the key performance indicators.

In the section 3 pilots are explained and evaluated in details. As evaluation methodologies and tools we have considered: questionnaires, qualitative interviews, co-creative workshops and real life testing – pilot tests. Input for the evaluation process comes from: platform architecture, mechanisms and tools to be tested by citizens, defined KPIs and involved target groups. Output from the evaluation process will allow other WPs to identify missing or improvable functionalities and improve the solutions that will be integrated in the final pilots. In addition, feedback of the end-uses will enable improvement of developed APIs (as part of WP4) and to foster engagement of the different communities to the Sociotal concept (as part of WP6). Two pilots are presented, namely Santander and Novi Sad pilots. Santander pilot aims to provide citizens with a platform that allows them sharing information produced by them only with people to whom they give permission. Novi Sad pilot implements two different pilot trials: Elevator Supervisor and Mood of the city. Appropriate test cases and evaluation methodologies are given in details.

References

[1] SOCIOTAL FP7 STREP EU project. Official Deliverable D3.2.1, " D3.2.1 Privacy-aware context-sensing device discovery"
[2] SOCIOTAL FP7 STREP EU project. Official Deliverable D3.3, "D3.3 Secure group communication "
[3] Mit Mood Meter, http://moodmeter.media.mit.edu/ , accessed 31.10.2014
[4] Anna Maffioletti,Agata Maida, Francesco Scacciati, "More Terminological and Methodological Problems in Measuring Happiness, Life Satisfaction and Well-Being: Some First Empirical Results", The Pursuit of Happiness and the Traditions of Wisdom SpringerBriefs in Well-Being and Quality of Life Research 2014, pp 13-21
[5] Peter Hills, Michael Argyle, The Oxford Happiness Questionnaire: a compact scale for the measurement of psychological well-being, Personality and Individual Differences Volume 33, Issue 7, November 2002, Pages 1073–1082
[6] Howarth, E., & Hoffman, M. S. (1984). A Multidimensional Approach to the Relationship between Mood Weather. British Journal of Psychology, 75 and (1), 15-23.
[7] CITI-SENSE FP7 EU project. Official Deliverable D8.2., "Pilot studies platforms"
[8] SOCIOTAL FP7 STREP EU project. Official Deliverable D4.1, "Feature specification of intuitive user and developer environment"
[9] Raspberry-Pi platform [Online]. Available: http://www.raspberrypi.org/ , Feb. 7,2014
[10] https://learn.adafruit.com/pir-passive-infrared-proximity-motion-sensor
[11] E.T. Hall. 1966. *The hidden dimension*
[12] EU FP7 USEMP Project. User empowerment for Enahnced Online Management. http://www.usemp-project.eu
[13] EU FP7 IoT Lab Project. Researching crowdsourcing to extend IoT testbed infrastructure for multidisciplinary experiments, with more end-user interactions, flexibility, scalability, cost efficiency and societal added value. http://www.iotlab.eu.
[14] SOCIOTAL FP7 STREP EU project. Official Deliverable D3.1.1, "D3.1.1 Device centric enablers for privacy and trust"
[15] SOCIOTAL FP7 STREP EU project. Official Deliverable D5.2, " D5.2 SOCIOTAL evaluation"
[16] SOCIOTAL FP7 STREP EU project. Official Deliverable D1.1, " D1.1 SOCIOTAL scenarios and requirements definition report"
[17] http://www.santandercitybrain.com/web/que_es_santandercitybrain, Dec. 16, 2014
[18] SOCIOTAL FP7 STREP EU project. Official Deliverable D6.1, " D6.1 Report on first year community interactions and detailed dissemination strategy"
[19] Sonja Lyubomirsky, Heidi S. Lepper A Measure of Subjective Happiness: Preliminary Reliability and Construct Validation, Social Indicators Research, February 1999, Volume 46, Issue 2, pp 137-155
[20] PN Belhumeur, JP Hespanha, D Kriegman, Eigenfaces vs. fisherfaces: Recognition using class specific linear projection, Pattern Analysis and Machine Intelligence, IEEE Transactions on 19 (7), 711-720
[21] YALE Dataset Athinodoros Georghiades, Peter Belhumeur, and David Kriegman's paper, "From Few to Many: Illumination Cone Models for Face Recognition under Variable Lighting and Pose", PAMI, 2001
[22] http://docs.opencv.org/index.html

Abbreviations and acronyms

AA	Attribute Authority
AAA	Authentication, Authorization and Accounting
AC	Access Control
API	Application Programming Interface
CP-ABE	Ciphertext Policy Attribute-Based encryption
DISMAP	Accessible routes for Disabled People Navigator
DIY	Do It Yourself
F2F	Face to Face
GM	Group Manager
IDE	Integrated Development Environment
IoT	Internet of Things
IdM	Identity Manager
I2C	Inter-Integrated Circuit
KPI	Key Performance Indicator
NFC	Near Field Communications
PDP	Policy Decision Point
PIR	Passive Infrared
QR	Quick Response Code
REST	Representational State Transfer
RPI	Raspberry Pie
RSSI	Received Signal Strength Indication
SD	Secure Digital
SHS	Subjective Happiness Scale
SPI	Serial Peripheral Interface
TRL	Technology Readiness Level
XACML	eXtensible Access Control Markup Language