Multi-layered Security Technologies

for hyper-connected smart cities

D2.2: M-Sec pilots definition, setup and citizen involvement plan

March 2019

Grant Agreement No. 814917

Multi-layered Security technologies to ensure hyper-connected smart cities with Blockchain, BigData, Cloud and IoT

Project acronym	M-Sec
Deliverable	D2.2 M-Sec pilots definition, setup and citizen involvement plan
Work Package	WP2
Submission date	March 2019
Deliverable lead	Sonia Sotero (AYTOSAN) / Keiko Doguchi (NTTE)
Authors	Sonia Sotero (AYTOSAN), Arturo Medela (TST), Vanessa Clemente, Tomás García (WLI), Mathieu Gallissot (CEA), Sofia Esteves (F6S), Jin Nakazawa (KEIO), Keiko Doguchi (NTTE), Rui Tanabe (YNU), Aamir Bokhari (YNU)
Internal reviewer	Antonis Likte, Orfeas Voutyras (ICCS) / Kenji Tei (WU)
Dissemination Level	Public
Type of deliverable	R

The M-Sec project is jointly funded by the European Union's Horizon 2020 research and innovation programme (contract No 814917) and by the Commissioned Research of National Institute of Information and Communications Technology (NICT), JAPAN (contract No. 19501).

Version history	- V01, 13/November/2018, Sonia Sotero, Full ToC & initial Content. - V02, 27/November/2018, Sonia Sotero, Review after November GA. - V03, 20/December /2018, Sonia Sotero, EU contributions to pilots. - V04, 14/January/2019, Sonia Sotero, update on Use Cases' names & contributions to Use Case 2 pilots. - V05, 15/January/2019, Sonia Sotero, JP contributions to pilots. - V07, 28/January/2019, Sonia Sotero, update on Pilot 5.1 - V08, 31/January/2019, Arturo Medela, update on Pilots' definition from Use Case 1. - V09, 31/January/2019, Tomás García, update on Pilots' definition from Use Case 2. - V10, 1/February/2019, Jin Nakazawa, update on Pilots' definition from Use Case 3. - V11, 6/February/2019, Arturo Medela, more detailed definition of Pilots 1.1 & 1.2 and Use Case 6 summary. - V12, 7/February/2019, Sonia Sotero, integrated version & update on Pilot's definition, stakeholders engagement plan & set up from Use Case 1 and Pilot's definition & set up from Use Case 2. - V13, 13/February/2019, Arturo Medela & KEIO, input in Use Case 4 Pilot 4.1 and Use Case 6. - V14, 15/February/2019, Sonia Sotero, integrated version & update of Stakeholders engagement plan of EU Pilots. - V15, 18/February/2019, Arturo Medela, update on Pilot 1.2 and improved version of the content initially provided for Use Case 6. - V16, 22/February/2019, Vanessa Clemente, update on Use Case 2. - V17, 25/February/2019, KEIO, input in Use Case 4 Pilot 4.2. - V18, 25/February/2019, NTTE, input in Use Case5 Pilot 5.1. - V19, 25/February/2019, CEA, input in Ethics plans on EU and cross-border pilots. - V2, 22/February/2019, Sonia Sotero, integrated version to be reviewed. - V2.1, 27/February /2019, Kenji Tei, 1st internal review. - V22, 27/February /2019, Sofia Esteves, review. - V23, 27/February/2019, NTTE, input in stakeholders management plan on pilots 4.1& 4.2. - V24, 27/February/2019. Sonia Sotero, input in Use case5 pilot 5.1 and answers to some review comments. - V25, 27/February/2019. Vanessa Clemente, answers to some review comments. - V26, 27/February/2019, Orfefs Voutyras, internal review. - V27, 28/February/2019, Sonia Sotero, answers to some comments. - V28, 28/February/2019, Arturo Medela, answers to some comments on Pilots 1.1 and 1.2.

- V29, 01/March/2019, Rui Tanabe, update on planning and evaluation methodology in Use Case 4 Pilots 4.1 & 4.2.
- V30, 04/March/2019, Vanessa Clemente, answers to some comments.
- V31, 06/March/2019, NTTE, update on Use Case 4 Pilots 4.1 & 4.2.
- V32, 07/March/2019, Jin Nakazawa, answers to some comments on Pilots 3.1, 4.1, and 4.2.
- V33, 08/March/2019, Sonia Sotero, integrated version and answers to some review comments on Pilots 1.1 and 1.2.
- V34, 12/March/2019, NTTE, answers to comments on Pilot 5.
- V35, 12/March/2019, Vanessa Clemente, answers to comments on Pilot 2.
- V37, 12/March/2019, Jin Nakazawa, answers to comments on Pilot 3 & 4.
- V4, 13/March/2019, Sonia Sotero, integrated version for internal review.
- V4.1, 14/March/2019, Orfefs Voutyras, internal review.
- V4.2, 18/March/2019, Kenji Tei, internal review.
- V4.3, 19/March/2019, Jin Nakazawa, Arturo Medela & Mathiew Gallissot, resolution of comments.

Table of Contents

List of Tables

List of Figures

Glossary

AC	Alternating Current
APP	Application
BT	Bluetooth
GDPR	General Data Protection Regulation
GPS	Global Positioning System
GPU	Graphics Processing Unit
HTML	Hypertext Markup Language
HW	Hardware
ID	Identification
IDS	Intrusion Detection System
IoT	Internet of Things
IP	Internet Protocol
JSON	JavaScript Object Notation
KPIs	Key Performance Indicators
MAC	Media Access Control
MQTT	Message Queuing Telemetry Transport
MVP	Minimum Viable Product
NB-IoT	Narrow Band IoT
PIPA	Personal Information Protection Act
PM2.5	Particulate Matter 2.5
QR Code	Quick Response Code
SQL	Structured Query Language
SW	Software
T	Task
TCP	Transmission Control Protocol
TCP/IP	Transmission Control & Internet Protocols
TLS	Transport Layer Security
UDP	User Datagram Protocol

UV-A	Ultraviolet A
XML	Extensible Markup Language
XMPP	Extensible Messaging and Presence Protocol
WP	Work Package
Y	Year(s)

1 Introduction

The current document, deliverable 'D2.2 M-Sec pilots definition, setup and citizen involvement plan', provides the initial version of M-Sec pilots that will be developed in both pilot cities, Santander and Fujisawa, within the task 'Task2.2 – M-Sec: pilots definition, setup and citizen involvement'. In detail, it presents the IoT infrastructure to be deployed as well as the corresponding application services, cloud infrastructure, and facilities. It also describes how it is planned to attract and engage end-users and stakeholders, while ensuring GDPR compliance. Additionally, pilot setup is defined, including details on how, when and where pilots will be set up, together with the KPIs that will enable the evaluation of the pilots.

A common approach has been adopted in the description of the pilots: each one of them includes a definition, a stakeholders' engagement plan, a data management plan, an ethics plan and, lastly, the setup description.

Finally, conclusions are reported in the last section of this document.

1.1 Relation to other WPs and Tasks

Task T2.2 receives input from WP2 tasks, in particular from 'Task2.1 – Use cases description' (which is in charge of identifying and describing use cases) and from 'Task2.4 - Overall system validation and evaluation' (which is in charge of the overall M-Sec system validation and evaluation). Additionally, this task is aligned to and receives input from Task 5.3 on GDPR compliance in order to include such input in the different stages of each pilot. At the same time, task T2.2 provides its outcomes to 'WP3 – Requirements, architecture for hyper connected smart cities', in particular in 'Task3.1 – System level and User level requirements' where M-Sec requirements are defined and consolidated, and also, in 'Task3.2 – M-Sec architecture', where the M-Sec architecture will be defined.

1.2 Methodology followed

In order to enable the M-Sec paradigm, the project will research and implement a multi-layered architecture offering its reference implementation for validation and demonstration purposes. The work to be done during the project lifetime will be divided in two main areas: research activities on the development of the M-Sec platform and demonstration activities regarding pilots to be carried out in both pilot cities.

These demonstration activities are the core of WP2, which includes the validating pilots and how they are going to be implemented, the final integrated and validated M-Sec prototype, and its evaluation in real environments and from real users. The main objective of these pilots is to test and validate the M-Sec architecture and platform, ensuring that technological developments meet cities needs and allowing M-Sec's results to be exploited not only to develop but also to offer new Smart City applications and services.

Additionally, these pilots will ensure the project meets its main objectives (in particular Objective 4), as it can be seen in the following table.

Table 1-1: M-Sec KPIs for pilots

Objective 4: Future decentralised IoT ecosystem		
Objectives/Sub-objectives	Key Performance Indicators	Minimum target
4.1 Developing a novel marketplace where smart objects can exchange, information, energy and services through the use of virtual currencies	• Smart objects joining in the market • Total exchange of virtual currencies for virtual goods trade via the marketplace	1,000 10,000
4.2 Creating demonstrators and ecosystems for real-life use cases	• Number of demonstrators • Number of use cases per demonstrator	4 (2 per city) 2
4.3 Developing innovative ideas through the involvement of new entrants	Applications built with the new ideas during the project lifetime	5

Finally, it is important to point out that this deliverable contains a first version of the definition of the pilots, which will be concreted in the following deliverables of this WP: D2.3 (M24) and D2.4 (M36). Additionally, any modification of the pilots will be included in those deliverables.

2 M-Sec pilots

This section provides a detailed description of the pilots that will be developed in Europe and Japan, concretely in Santander and Fujisawa, in order to validate use cases described in D2.1.

It is important to highlight that the development and test of a successful pilot mean finding a balance between the needs of the different participants including project, cities, stakeholders and potential end users.

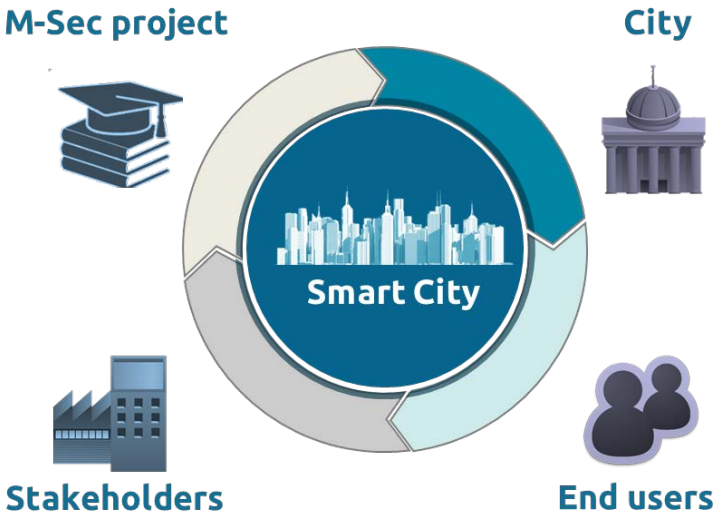

Figure 2—1: Main participants in M-Sec pilots

From the project perspective, the objective of these pilots is to test and validate use cases described in D2.1 in a real environment. This is a research objective which dictates the technology chosen to implement the pilots, their design to generate the data needed to validate the hypothesis, and, also their evaluation.

From the city point of view, one of the main goals is to improve the quality of life not only of citizens, but also of tourists using technology as a tool. In this sense, a fundamental pillar within this improvement is the optimisation of public services.

End users want to benefit from the new solutions/services/apps in a simple way and without requiring specific technological knowledge. As it will be explained later, it is important to take into account the existing technological gap and adapt our pilots to people needs. That is why different meetings will be organised within the lifetime of pilots.

Last but not least, stakeholders sometimes miss being heard or involved, therefore, we may lose valuable information and, above all, lessons learnt. In this sense, we consider co-design mechanisms and focus groups as tools to leverage that knowledge.

Taking into account the aforementioned approach, nine pilots will be carried out in total in the pilot cities, in order to validate the six use cases defined in deliverable D2.1:

- Four pilots will be carried out in Santander,
- Three pilots will be carried out in Fujisawa,
- Two cross-border pilots will be carried out in both Santander and Fujisawa.

The following table summarises the pilots to be carried out in the pilot cities.

Table 2-1: M-Sec pilots

Use cases	Pilot (s)	Pilot's names	City
Use Case 1	Pilot 1.1	Reliable IoT environmental data devices with multi-layered security for a smart city	Santander
	Pilot 1.2	Reliable IoT crowd counting data devices with multi-layered security for a smart city	Santander
Use Case 2	Pilot 2.1	Home Activity Tele-assistance	Santander
	Pilot 2.2	Social & Physical Wellbeing	Santander
Use Case 3	Pilot 3.1	Secure Mobile Environment Sensing	Fujisawa
Use Case 4	Pilot 4.1	Privacy-secure Garbage Counting	Fujisawa
	Pilot 4.2	Secure Affective Participatory Sensing of City Events	Fujisawa
Use Case 5	Pilot 5.1	A marketplace of IoT services for effective decision making	Fujisawa & Santander
Use Case 6	Pilot 6.1	Citizen as sensor	Santander & Fujisawa

Finally, due to the uniqueness of the different pilots, a common approach has been adopted with the aim of homogenising them. Each one of them follows the same structure:

- Definition: including the goals, location, and infrastructure.
- Stakeholders engagement plan: identifying not only stakeholders but also end users, and describing how they will be recruited.
- Data management plan: describing the types and format of the data to be used as well as the methodology to be followed for their management.
- Ethics plan: describing how compliance with ethical issues has been ensured.
- Setup: including the planning and the evaluation methodology.

2.1 Use Case 1: Reliable IoT devices with multi-layered security for a smart city

This section describes how Use Case 1 will be tested through two pilots that will be carried out in Santander: the first one is related to environmental data and the second one to crowd counting.

2.1.1 Pilot 1.1

2.1.1.1 Definition

The main idea behind this pilot consists in deploying IoT devices offering environmental data (mainly temperature, humidity, noise, and illuminance measurements) and looking for citizens' involvement through them leaving their opinion about that data by employing a 5-star rating or a similar method.

On a first approach, to ensure users involvement, a series of QR codes could be stuck close to the place where every IoT device is located, guiding the users to a specific webpage where they could check the measurements in real time and provide their rating.

Nevertheless, the goal here consists in achieving steps forward with regard to security measurements and citizen involvement. The former will be achieved from both a HW and a SW approach, also linked to the application of blockchain techniques, while the latter will be linked to the implementation of gamification functionalities and rewarding mechanisms.

Regarding citizen's involvement, it is important to take into account that Santander is nowadays an international reference within Smart Cities due to the combination of two factors: the active participation in European research projects that turn the city into a city lab, and the development of different city initiatives which allow managing city services more efficiently. In this sense, in recent years citizens have grown accustomed to testing and enjoying different applications related to Smart City concepts; therefore the consortium must look for something really innovative and attractive to get their attention. As a first approach, we could define some route/itinerary within the city, and combine environmental data with other information of a park, such as flora, fauna, or iconic places information, to show it to the citizens in a user-friendly way.

In this sense, during a meeting with municipal heads of the environmental service, it was decided that this pilot project should be carried out in one of the city's parks. Therefore, after an analysis of the different parks, the park of Las Llamas was recommended as the perfect location for such a pilot due to several reasons. Firstly, this park is located near some of the most stunning beaches downtown and is close to many university faculties. Secondly, in that area it is possible to engage in sports, attend concerts in *Escenario Santander*, carry out leisure and entertainment activities, enjoy the bicycle lane, rent or leave the municipal bicycles, take a walk along the footbridges of the park's pond or spend time with the children in children's areas. Additionally, it has a huge wetland with more than 2500 trees, inhabited by different types of birds and amphibians. In late summer and early fall, migratory birds gather here, during their journey from the north to the south of Europe. Finally, there are specific routes defined within this park. For example, the Santander City Council invited elementary and primary schools to learn more about the wetland in the park of Llamas and the species that can be found there, through educational and environmental awareness tours

on the World Wetlands Day. Further information is available in the following link (http://santander.es/noticia/parque-llamas-aves-habitan-centran-actos-del-dia-humedales).

Therefore, we could base and enrich with the environmental information one of the existing routes in some way that fits in the project and is useful for the city. This route could include a series of stops (1, 2, etc.) where the user could acquire this visualised information.

Figure 2—2: Park of Las Llamas in Santander

Therefore, M-Sec could offer users an app or website that guides them, in a nice and intuitive way, through fixed routes, as suggested by the Municipality, enriching them with different types of information (e.g. trees in the surroundings, birds migrating to and living in the different zones of the park) and the environmental measurements provided by the IoT devices deployed as part of the pilot.

In terms of gamification and to encourage wider participation, the consortium will define a prize for those who finish or pass through several points of the route. Thus, M-Sec will track users, should they give their consent, and if and when they complete the suggested route they will receive a token.

All in all, this pilot could also be linked to the M-Sec marketplace, based on the blockchain, and store IoT data produced by the sensors developed. Its main features are recapped in Table 2-2 below.

Table 2-2: M-Sec Use Case 1 Pilot 1.1 details

Pilot name	Reliable IoT environmental data devices with multi-layered security for a smart city
Location of the pilot	Santander City (Spain)
Infrastructure	• IoT sensing devices • Secure data delivery platform • Environment monitoring and route guiding application
IoT sensors	• Temperature, humidity, noise, illuminance

2.1.1.2 Stakeholders engagement plan

The first step to get major engagement consists in developing a proper and user-friendly app or website which will capture citizens' attention.

We will collaborate with the Municipal Department of Environment in order to define not only the routes but also the information to be shown in the app/website. Once the app or website is designed, we will look for friend-users, including municipal staffs and also citizens that have shown an interest in taking part in these kinds of experiences in the past, who are involved in testing this new tool and in providing feedback. Based on our experience in other European projects, it is more efficient to start testing with a small initial number of users.

Once the initial testing stage has passed, the app/website will be promoted more widely, not only via the local media channels reachable by the consortium members (e.g. local mass media, web pages, newsletters, and/or social media accounts) but also by holding dedicated workshops with potentially interested stakeholders. For instance, if we choose as a target audience the students of elementary and primary schools, we could collaborate with the Department of Education and school principals to promote the use of the app or webpage.

2.1.1.3 Data management plan

The following table shows a summary of the data management plan.

Table 2-3: M-Sec Use Case 1 Pilot 1.1 data management plan

Type of data	• Raw values from sensors related to Celsius degrees, humidity percentage, as well as dB and lux measurements.
Format of data	• UDP packets using a defined framework.
Data collection	• Over the course of the pilot, data will be generated from sensors, and be collected and forwarded from the NB-IoT (Narrow Band IoT) devices via UDP in the format defined.
Data storage	• Over the course of the pilot, data will be collected and entered into a SQL database.
Data management	• All the data generated during the pilot will be deleted. Before their elimination, the pilot evaluation report will generate anonymous and aggregated views of the data to illustrate the pilot actions and results aligned to the defined KPIs.
Data Management Principles	• The anonymity and privacy of participants must be respected. Personal information must be kept confidential. Guarantees of confidentiality and anonymity given to the participants must be honoured, unless there are clear and overriding reasons to do otherwise.

- In case the participants must be registered at the M-Sec platform and the pilot clients, they must not be registered with their name, but through using e.g. an ID-code instead.
- All researchers have the duty of confidence in regard to collected data.
- The integrity of stored, processed and published data must be ensured by the researchers and the project consortium.
- Data that are collected by the participant at the M-Sec platform must be treated with care.
  - The participants must be informed that the data could be used for the project.
  - The participants must be informed in which way the data could be used.
  - The participants must be informed who has the data sovereignty.
  - The participants must be informed when the collected data will be deleted.
  - Appropriate measures must be taken by the researchers to protect the collected data.
  - Appropriate measures must be taken by the researchers to store and process data in a secure manner.
  - In case the participant withdraws from the pilot before it ends, the collected data at the platform must be deleted or the access to them must be impossible for others, without any undue delay.

2.1.1.4 Ethics plan

In this pilot, participants self-register themselves using a pointer (QR Code, etc.) in public space. When they do self-register, they are notified about the data management principles as detailed in the previous section. Participants will have a right to retract anytime within the application and, when they do, all relative data to the participant will be deleted, except for those used to generate KPIs. In practice, all partners hosting data related to a participant will be notified about the wish of the participants to withdraw and must then perform the deletion of the data.

By default, all data related to participants will be deleted at the end of the project. Each partner treats data with confidentiality in their information system with accountability for accessing and manipulating those data within their organisation.

2.1.1.5 Set up

The pilot will be set up mainly by the consortium members located in Santander, assisted and following the recommendations made by the corresponding municipality officers in different areas such as industrial engineering and environment areas. We will collaborate to define the best spots to install the IoT devices which will feed the pilot both from a technical (requirements of IoT devices) as well as city point of view. A summary of this pilot set up is shown in the following table.

Table 2-4: Use Case 1 Environmental data Pilot set up

Planning	• **Start Date:** M21 (March 2020) • **Duration:** M21 – M36 (15 months) • **Phases:** o **PHASE 1 – Main features set-up** (M15-M18): Preparation of the agreed solution. o **PHASE 2 – Initial tests** (M18-M21): Sensors installation & calibration. Connectivity tests. Front-end applications tests. Proof-of-Concept oriented. o **PHASE 3 – 1st Trial of the pilot** (M21): Integration with the M-Sec platform. Iterative sub-releases. o **PHASE 4 – 2nd Trial of the pilot** (M33): Iterative sub-releases. o **PHASE 5 – Pilot Evaluation** (M33-M36): Questionnaires. KPIs follow-up report.
Environmental data setup	• In this pilot, citizens and municipality representatives participating in the pilot will be able to install in their smartphones a mobile app featuring the suggestion of interesting routes in Las Llamas Park. This client front-end will be presenting data related to environmental measurements and other sources of park information. • A gaming feature will be integrated on the mobile app allowing users to apply for participation and obtain rewards.
Evaluation methodology	• **KPIs** o # downloads / # web access hits o # participants o # participants on the proposed game • **Surveys** o Two surveys to be conducted about satisfaction level - During 1st release - Final evaluation

2.1.2 Pilot 1.2

2.1.2.1 Definition

The main idea behind this pilot consists in deploying IoT devices capable of detecting BT/Wi-Fi signal from cell phones and offering a precise figure related to the number of people present at a certain time in a designated spot. So far, these devices present as a feature the ability to keep the history of the number of people that were at those spots during the measurement times. In addition, the proposed solution is capable of tracking the movement of people around the area of study, following the MAC Wi-Fi signals of their cell phones, while keeping intact their privacy.

So far, the main scenarios considered are near downtown beaches in Santander and certain parking places close to them. Parking lots are left aside since many people leave their car parked there and go to the beach on foot, therefore the detection will not be reliable.

Nevertheless, having in mind these devices can act as crowd-counters, they could be used not only in downtown beaches but also in areas such as the Park of Las Llamas (see Figure 2—3), complementing the activity carried out as part of Pilot 1.1. In addition, it would also be useful in other areas that, during summertime, are crowded. Therefore, the IoT devices to be designed should be portable so that they can be placed into those diverse spots at different times.

Figure 2—3: Another view of the Park of Las Llamas in Santander

Once again, the challenge here is to achieve an improvement in security features, which will be implemented via HW and SW, and obtain the approval of users and high participation in the pilot. To manage that, an application that makes the development attractive and useful for end users must be designed. When dealing with the Park of Las Llamas there are already some defined routes, as discussed in the Pilot 1.1. The M-Sec pilot could enrich the information currently offered there by adding data related to the number of persons at different stops in that route, as well as keeping historical data related to the number of visitors in each stop and helping municipal services detect which are the spots preferred by visitors.

Table 2-5: M-Sec Use Case 1 Pilot 1.2 details

Pilot name	Reliable IoT crowd counting data devices with multi-layered security for a smart city
Location of the pilot	Santander City (Spain)
Infrastructure	• IoT sensing devices • Secure data delivery platform
IoT sensors	• **Counter sensors**: cell phones BT/Wi-Fi signal detection

2.1.2.2 Stakeholders engagement plan

Similarly and tightly related to what is proposed in Pilot 1.1, the initial step to get major engagement of end users consists of offering citizens a functionality that captures their attention. Marketing techniques will be used in the development of the messaging to be shown, and the app will be optimised taking into account a good User Interface and User Experience, for positive interactivity.

In this pilot, we are able to collaborate with the municipal tourist service, in charge of the current route through the park of Las Llamas. As in the previous pilot, once this functionality is agreed upon, we will look for friend-users, including municipal staff and also citizens that have shown an interest in taking part in these kinds of experiences in the past, who will test and evaluate this functionality. Finally, and taking into account the received feedback, we will promote it properly and widely, not only via the local media channels reachable by the consortium members (e.g. web pages and/or social media accounts) but also by holding dedicated workshops with potential interested stakeholders. Collaboration with municipal services related to tourism, environment and citizen participation to promote it is foreseen.

2.1.2.3 Data management plan

The following table shows a summary of the data management plan.

Table 2-6: M-Sec Use Case 1 Pilot 2 data management plan

Type of data	• Raw data from the sensors, which will make a count of the number of signals detected and deliver an integer number.
Format of data	• TCP packets using a defined framework.
Data collection	• Over the course of the pilot, data will be generated from sensors, and be collected and forwarded via TCP in the format defined.
Data storage	• Over the course of the pilot, data will be collected and entered into SQL database.
Data management	• All the data generated during the pilot will be deleted. Before their elimination, the pilot evaluation report will generate anonymous and aggregated views of the data to illustrate the pilot actions and results aligned to the defined KPIs.
Data management principles	• The anonymity and privacy of participants must be respected. Personal information must be kept confidential. Guarantees of confidentiality and anonymity given to the participants must be honoured, unless there are clear and overriding reasons to do otherwise. • In case that the participants must be registered at the M-Sec platform and the pilot clients, they must not be registered with their name. E.g. an ID-code will be applicable instead of it. • All researchers have the duty of confidence in regard to collected data. • The integrity of stored, processed and published data must be ensured by the

researchers and the project consortium.

2.1.2.4 Ethics plan

In this pilot, participants self-register themselves using a pointer (QR Code, etc.) in public space. When they do self-registration, they are notified about the data management principles as detailed in the previous section. Participants will have a right to retract anytime from the application and when they do, all relative data to the participant will be deleted, except for those used to generate KPIs. In practice, all partners hosting data related to a participant will be notified about the willingness of the participants to withdraw and must then perform the deletion of the data. By default, all data related to participants will be deleted at the end of the project. Each partner treats data with confidentiality in their information system with accountability for accessing and manipulating those data within their organisation.

2.1.2.5 Set up

Once again, the pilot will be set up mainly by the consortium members located in Santander, assisted and following the recommendations made by the corresponding municipality officers in the domains of tourism and environment. In collaboration with them, the best spots to install the IoT devices which will feed this pilot will be defined, taking into account technical and city perspectives. A summary of this pilot set up is shown in the following table.

Table 2-7: Use Case 1 Crowd Counter Pilot set up

Planning	• **Start Date:** M21 (March 2020) • **Duration:** M21 – M36 (15 months) • **Phases:** o **PHASE 1 – Main features set-up** (M15-M18): Preparation of the agreed solution. o **PHASE 2 – Initial tests** (M18-M21): Sensors installation & calibration. Connectivity tests. Front-end applications tests. Proof-of-Concept oriented. o **PHASE 3 – 1st Trial of the pilot** (M21): Integration with the M-Sec platform. Iterative sub-releases. o **PHASE 4 – 2nd Trial of the pilot** (M33): Iterative sub-releases. o **PHASE 5 – Pilot Evaluation** (M33-M36): Questionnaires. KPIs follow-up report.
Crowd counting data setup	• In this pilot, citizens and municipality representatives participating will be able to check the number of total cell phones with a BT/Wi-Fi connection active at a certain spot, which will help to infer the number of persons located there. • No actual action will be derived from the collection and analysis of presence data from detected devices. The City of Santander will be collecting the data but only for information purposes.
Evaluation methodology	• **KPI** o # detections • **Surveys**

- Two surveys to be conducted about satisfaction level
  - During 1st release
  - Final evaluation

2.2 Use Case 2: Home monitoring & Wellbeing Tele-assistance for active and independent ageing people

This section describes how Use Case 2 will be tested through two pilots that will be carried out in Santander: the first one focuses on tele-assistance service and the second one on wellbeing.

2.2.1 Pilot 2.1

2.2.1.1 Definition

Pilot 2.1 'Home Activity & Emergencies' will be piloted by digitalising some of the current analogic-based, tele-assistance service provided by Social Services department from Santander City Council through a third party operator. This service digitalisation will enable the applicability of M-Sec services to the different elements that compound the service (IoT home sensor devices, communication and connectivity, data protection and user/service authentication).

Surveys included in D2.1 indicated that 75% of the potential users are older than 81 years and most of them are not accustomed to using new technologies in their daily lives. Therefore, it was decided to select those functionalities of the telecare service that do not involve a person-device interaction and, at the same time, do not generate an immediate reaction on the part of the company in charge of managing the telecare service.

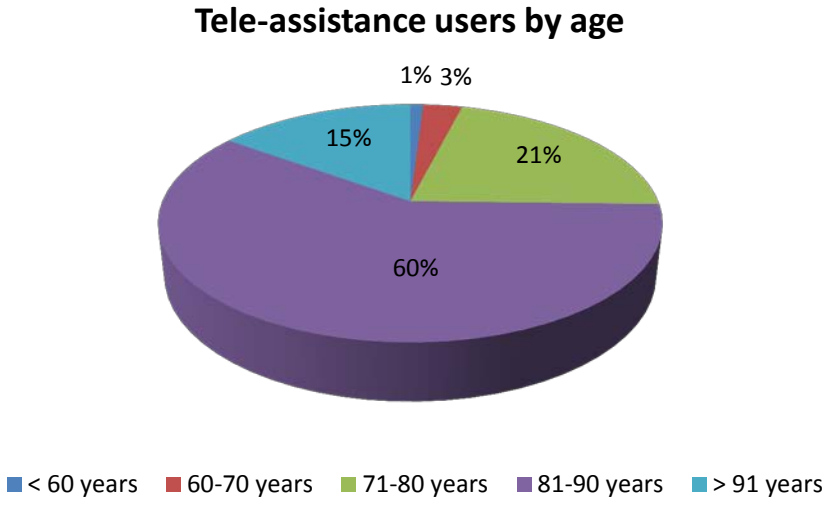

Figure 2—4: Tele-assistance service users by age

The main goals designed for the system (tele-assistance service + M-Sec platform) that will be probed during the execution of the pilot will be:

- Improvement of quality of life of elderly people who live alone and are not familiar with the use of new technologies.
- Creation of a network of caregivers, formed by relatives or neighbours previously authorised by the elderly, who will be able to check users' status thanks to the combination of the measured parameters.
- Improvement of data gathering and information enrichment with the digital transformation of the current local tele-assistance & emergencies social service provided by the city government, through the introduction of digital sensors and communications.
- Improvement of data security and integrity through the use of M-Sec layers in the different elements that compound the service. For example, components (sensors, IoT devices, cloud systems) involved in the data stream dissemination need to be tamper-proof to prevent malicious attacks on devices.
- Data collected from IoT sensors must be authenticated as provided by the monitored subject to assure data proof-of-ownership at the application level.

The following table describes briefly the main aspects of the pilot execution.

Table 2-8: Use Case 2 pilot 2.1 details

Pilot name	Home Activity Tele-assistance
Location of the pilot	Santander City (Spain)
Users	• 5 users older than 65 years old. • Family relatives and/or other actors (friends, neighbours, community members) willing to participate as a care giving network and social contact for the elderly citizen. • Acceptance and consent to participate in this pilot under the conditions expressed by the M-Sec consortium.
Infrastructure	• IoT Sensors and gateways • Web front-end displaying enriched monitoring & emergency data from users • Family caregivers will be given an app to access the elder granted data
Home sensors	• **Connectivity Hub (Gateway):** to collect data from sensors (ZigBee) • **Presence sensor:** to detect human presence in a room • **Window/door open sensor:** to detect home doors/windows opening • **Temperature sensor:** to detect room temperature • **Smart plug:** to detect activity in home appliances (e.g. TV)
Tele-service provider and care giving network	• **M-Sec Tele-assistance** and care giving network **Dashboard**: access to web app dashboard for the monitored users. Additionally, WLI will also have access to this dashboard, in order to check and solve events.

2.2.1.2 Stakeholders engagement plan

In collaboration with the Social Services department from Santander City Council and the company in charge of managing the telecare service we will tackle the task of identifying potential friend users who should meet the following profile:

- be users of the telecare service, therefore elderly people,
- be interested in participating in the pilot and
- having a family member or neighbour who also wants to be part of the network of caregivers.

Once the dashboard is ready and privacy issues are taken into account, a dedicated meeting with each potential friend user and their family member or neighbour will be organised, in order to present them the pilot and invite them to participate to it. During these meetings, the users shall be provided with and requested to provide all necessary information to start with the pilot. A dedicated team will pay close attention to the explanation of the processes involved in a simplified manner to everyone involved, especially to elderly people.

2.2.1.3 Data management plan

The following table shows a summary of the data management plan.

Table 2-9: Use Case 2 Pilot 2.1 data management plan

Type of data	• Raw data values from sensors (temperature, voltage, frequency, ON/OFF values, timestamp, etc.) • Metadata associated with raw data (network link strength, AC frequency, sensor type, data unit type, transaction type, etc.)
Format of data	• JSON data exchange format for transporting data & metadata within an MQTT channel. • Metadata will be generated to describe the data generated sensors and patient's home and will be stored alongside the data. Appropriate metadata standards will be applied during the creation of the metadata.
Data collection	• Over the course of the pilot, data will be generated from sensors, and be collected and forwarded via MQTT by a Gateway Hub device in JSON format. • MQTT channels will be created upon the different measurements collected by the home sensors. • The Tele-assistance back-end will subscribe to all these MQTT channels for each user to receive all the data from every home.
Data storage	• Over the course of the pilot, data will be collected and entered into NoSQL database (MongoDB) as JSON documents.
Data management	• This pilot will generate data to be displayed at the Tele-assistance operator to monitor elderly homes. • The generated data will be processed to enable alert triggering when values

	go over pre-defined values deemed dangerous for the monitored patient. • All the data generated during the pilot will be deleted. Before their elimination, the pilot evaluation report will generate anonymous and aggregated views of the data to illustrate the pilot actions and results aligned to the defined KPIs.
Data management principles	• Survey data will be generated only in an anonymised form. Therefore, the questionnaires, interview guidelines and other used instruments must not contain questions of which the answers could lead to the participant's identity – alone or in combination with other answers. • The anonymity and privacy of participants must be respected. Personal information must be kept confidential. Guarantees of confidentiality and anonymity given to the participants must be honoured, unless there are clear and overriding reasons to do otherwise. • In case the participants must be registered to the M-Sec platform and the pilot clients, they must not be registered with their name. Instead, an e.g. ID-code could be used. • The participants themselves have their data sovereignty. In the case the participant wants the deletion of their data, this has to be done without any undue delay. • The participant is allowed to change/ limit the access authorisation of their data collected at the M-Sec platform and the pilot clients. • Only information pertinent to piloting activities is permitted to be collected. • All researchers have the duty of confidence in regard to collected data. • The integrity of stored, processed and published data must be ensured by the researchers and the project consortium. • Participants' data collected by the M-Sec platform must be treated with care. o Participants must be informed that the data could be used for the project. o Participants must be informed in which way the data could be used. o The participants must be informed who has the data sovereignty. o The participants must be informed when the collected data will be deleted. o Appropriate measures must be taken by the researcher to protect the collected data. o Appropriate measures must be taken by the researcher to store and process data in a secure manner. o In case the participant withdraws from the pilot, the collected data at the platform must be deleted or the access to them must be impossible for others, without any undue delay.

2.2.1.4 Ethics plan

In this pilot, personal data are generated about the participants. In order to adopt the right strategy for the protection of the rights and freedom of individuals (meaning freedom for individual to make choices and to control how and with whom they share data collected by sensors), we first propose to perform a Data

Privacy Impact Assessment (DPIA) as defined by the GDPR. This DPIA will be built during the definition of the architecture and will assess the risk related to the privacy of the data.

In addition, some principles resulting from the philosophy of "privacy by design" will be adopted in coherence with the feasibility of the scenarios:

- Only the data necessary for the conduct of the experiment will be collected.
- The personal information will be on a database with restricted access to the partners with strictly necessary.
- A strict application of the principles of accountability and transparency to users will be adopted.

2.2.1.5 Set up

A summary of this pilot set up is shown in the following table.

Table 2-10: Use Case2 Pilot 2.1 set up

Planning	• **Start Date:** M21 (March 2020) • **Duration:** M21 – M36 (15 months) • **Phases:** o **PHASE 1 – User Panel set-up** (M15-M18): End users selection & training. User consent. o **PHASE 2 – MVP release** (M18-M21): Sensors installation & calibration. Connectivity tests. Front-end applications tests. Proof-of-Concept oriented. o **PHASE 3 – 1st Trial of the pilot** (M21): Integration with the M-Sec platform. Iterative sub-releases. o **PHASE 4 –2nd Trial of the pilot** (M33): Iterative sub-releases. o **PHASE 5 – Pilot Evaluation (M33-M36)**: Questionnaires. KPIs follow-up report.
Home set-up	• Elderly homes will be set-up with different sensors and gateways connected to the M-Sec platform. • All participating users will be informed of the pilot goals, duration and activities and their consent will be required. • Every participant will be provided with a sensor pack that may differ from one another. They will all contain a gateway hub for sensor connectivity. • Although all sensors may be deployable and installed by the monitored user, taking into account their age and specific profile, the consortium will be in charge of the deployment and installation. • The Tele-assistance company and care giving network will be provided with a web front-end displaying enriched monitoring & emergency data from users.
Evaluation methodology	• **KPI** o # alarms triggered o # data generated/day

- # tele-assistance actions
- # users
- # parameters to measure

- **Surveys**
  - Two surveys to be conducted about satisfaction level
    - During 1st release
    - Final evaluation

2.2.2 Pilot 2.2

2.2.2.1 Definition

In this pilot, elderly citizens and the caregiving network will be provided with a mobile app featuring communication capabilities to fight social exclusion and isolation (chat, video-chat and call). This client front-end will be managing wellbeing data related to a physical and mental activity.

The main goals designed for the system (well-being service + M-Sec platform) that will be probed during the execution of the pilot will be:

- Although Santander municipality is working to promote activities aimed at the elder people, sometimes communication is not as effective as expected. For this reason, the development of an app or web which provides information about specific activities and initiatives for older people may establish a communication channel that has not been tried so far.
- Strengthen the personal relationships of the elderly so that they have more social interactions and, at the same time, create new groups of people over 65, enabling them to participate to the community life of their environment.
- The elderly citizen will have two different networks: one for the people of their trust (family, friends, volunteers, neighbours, etc.), and that created thanks to the new app that will show dedicated activities and initiatives for elderly people.

The following table describes briefly the main aspects of the pilot execution.

Table 2-11: Use Case2 Pilot 2.2 details

Pilot name	Social & Physical Wellbeing
Location of the pilot	Santander City (Spain)
Users	A new set of users will be selected from those elderly citizens living in Santander with a profile matching the following aspects: • Elderly citizens (above 65) living alone and owning a smartphone. • Family relatives and/or other actors (friends, neighbours, community members) willing to participate as a care giving network and social contact for the elderly citizen. • Acceptance and consent to participate in this pilot under the conditions

	expressed by the M-Sec consortium.
Infrastructure	• Wellbeing devices to be provided to users • Users should have a mobile phone with an internet connection o Mobile app for smartphones that will feature a communication channel (chat, video-call, call)) to address their beloved ones.
Wellbeing devices	• Smart watch/bracelet to capture walking activity and sleep quality.
Caregiving network	• Family member, neighbours, friends to participate as part of the elder caregiving network will download the caregiving app and sign in as granted members.

2.2.2.2 Stakeholders engagement plan

The recruitment of potential friend users will take place in collaboration with municipal civic centres and municipal tele-centres, where different types of activities and initiatives are organised.

As in the previous pilot, once the mobile app is ready and any privacy issues are dealt with, dedicated meetings with potential friend users and their family members or neighbours will be organised, in order to present to them the pilot and invite them to participate to it. During these meetings, they shall be provided with and requested to provide all necessary information to start with the pilot.

Taking into account the received feedback, we could promote it properly and widely, not only via the local media channels reachable by the consortium members (e.g. web pages and/or social media accounts) but also by holding dedicated workshops with potential interested stakeholders.

2.2.2.3 Data management plan

The following table shows a summary of the data management plan.

Table 2-12: Use Case 2 pilot 2.2 data management plan

Type of data	• Raw data values from watch (steps, sleep time, etc.) • Metadata associated with raw data (sensor type, data unit type, transaction type, etc.)
Format of data	• JSON data exchange format for transporting data & metadata. • Metadata will be generated to describe the data generated sensors and patient's home and will be stored alongside the data. Appropriate metadata standards will be applied during their creation.
Data collection	• Over the course of the pilot, data will be generated from sensors and be collected and forwarded via watch device in JSON format via TCP/IP.
Data storage	• Over the course of the pilot, data will be collected and entered into NoSQL database (MongoDB) as JSON documents.

Data management	• This pilot will generate data to be displayed at the elder and caregiving network mobile app. • All the data generated during the pilot will be deleted. Before their elimination, the pilot evaluation report will generate anonymous and aggregated views of the data to illustrate the pilot actions and results aligned to the defined KPIs.
Data management principles	• Survey data will be generated only in an anonymised form. Therefore the questionnaires, interview guidelines and other used instruments must not contain questions, which answers could lead to the participant's identity – alone or in combination with other answers. • The anonymity and privacy of participants must be respected. Personal information must be kept confidential. Guarantees of confidentiality and anonymity given to the participants must be honoured, unless there are clear and overriding reasons to do otherwise. • In case that the participants must be registered at the M-Sec platform and the pilot clients, they must not be registered with their name. For example, an ID-code will be applicable instead. • The participants themselves have their data sovereignty. In the case the participant wants the deletion of their data, this has to be done without any undue delay. • The participant is allowed to change/ limit the access authorization of their data collected at the M-Sec platform and the pilot clients. • Only information pertinent to piloting activities is permitted to be collected. • All researchers have the duty of confidence in regard to collected data. • The integrity of stored, processed and published data must be ensured by the researchers and the project consortium. • Data that are collected by the participant at the MSEC platform must be treated with care. o Participants must be informed that data could be used for the project. o Participants must be informed in which way the data could be used. o The participants must be informed who has the data sovereignty. o The participants must be informed when the collected data will be deleted. o Appropriate measures must be taken by the researcher to protect the collected data. o Appropriate measures must be taken by the researcher to store and process data in a secure manner. o In case the participant withdraws from the pilot, the collected data at the platform must be deleted or the access to them must be impossible for others, without any undue delay.

2.2.2.4 Ethics plan

In this pilot, personal data are generated about the participants. In order to adopt the right strategy for the protection of the rights and freedom of individuals, we first propose to perform a Data Privacy Impact Assessment (DPIA) as defined by the GDPR. This DPIA will be built during the definition of the architecture and will assess the risk related to the privacy of the data. In addition, some principles resulting from the philosophy of "privacy by design" will be adopted in coherence with the feasibility of the scenarios:

- Only the data necessary for the conduct of the experiment will be collected.
- The personal information will be on a database with restricted access to partners.
- A strict application of the principles of accountability and transparency to users.

2.2.2.5 Set up

A summary of this pilot set up is shown in the following table.

Table 2-13: Use Case 2 pilot 2.2 set up

Planning	• **Start Date:** M21 (March 2020) • **Duration:** M21 – M36 (15 months) • **Phases:** o **PHASE 1 – User Panel set-up** (M15-M18): End users selection & training. User consent. o **PHASE 2 – MVP release** (M18-M21): Sensors installation & calibration. Connectivity tests. Front-end applications tests. Proof-of-Concept oriented. o **PHASE 3 – 1st Trial of the pilot** (M21): Integration with M-Sec platform. Iterative sub-releases. o **PHASE 4 – 2nd Trial of the pilot** (M33): Iterative sub-releases. o **PHASE 5 – Pilot Evaluation** (M33-M36): Questionnaires. KPIs follow-up report.
Wellbeing setup	• In this pilot, elderly citizens and caregiving network will be provided with a mobile app featuring communication capabilities to fight social exclusion and isolation (chat, video-chat and call). This client front-end will be managing wellbeing data related to a physical and mental activity. • Additionally, they will be also provided with a smartwatch to collect wellbeing data from their physical activity (steps, sleep, location) • Brief questions will be integrated on the mobile app allowing users to reply (e.g. Assistance to a public event, wellbeing questions).
Evaluation methodology	• **KPI** o # video calls o # calls o # wellbeing parameters o # data generated/day o # answer to questions

- # level of participation on public activities
- # users

- **Surveys**
  - Two surveys to be conducted about satisfaction level
    - During 1st release
    - Final evaluation

2.3 Use Case 3: Secure and Trustworthy Environment Monitoring with Automotive, Participatory and Virtual Sensing Techniques

This section describes how Use Case 3 will be tested through the pilot that will be carried out in Fujisawa.

2.3.1 Pilot3.1

2.3.1.1 Definition

This pilot study probes the power of multi-layered security mechanisms in the M-Sec platform, leveraging the mobile sensing platform that has been operated in Fujisawa city in Japan for three years. The IoT devices (sensors), the cloud system (servers of a sensor data exchange platform), and applications consuming sensor data streams included in the mobile sensing platform are extended with multiple security mechanisms. The IoT devices are secured by hardening and intrusion detection system. The former is achieved by existing best practices, such as closing unnecessary network ports. The latter is brought by the M-Sec project as one of the technical components developed as part of WP3. The traffic between the IoT devices and the cloud system is protected by the use of Transport Layer Security (TLS), which is a point-to-point encryption mechanism. In the cloud system, a sophisticated authentication mechanism is provided by the project in order to protect the data stream. In addition, end-to-end sensor data stream delivery is secured by a light-weight encryption mechanism and will be made configurable and manageable by a security management tool. These components will also be developed as part of WP3.

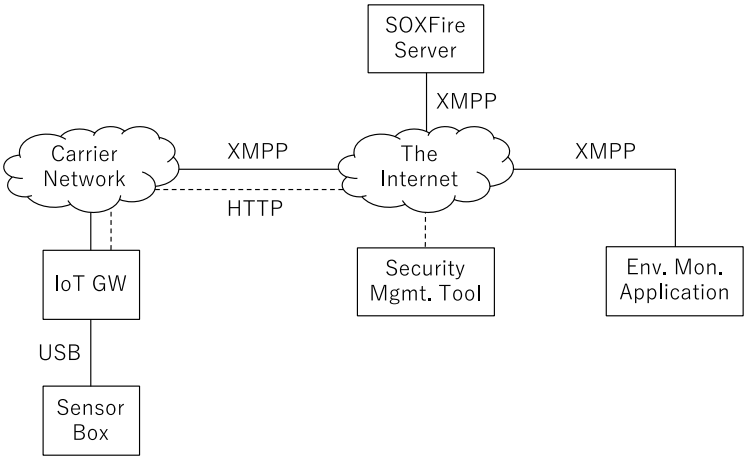

Figure 2—5: Topological overview of Use Case 3 Pilot 3.1

The pilot is planned to be held in Fujisawa city leveraging at least 10 garbage collection trucks that are part of the mobile sensing platform. It will last for 12 months during which we will evaluate the M-Sec platform and its technical components in terms of their effectiveness. The following table describes briefly the main aspects of the pilot execution.

Table 2-14: Use Case 3 pilot 3.1 details

Pilot name	Secure Mobile Environment Sensing
Location of the pilot	Fujisawa City (Japan)
Infrastructure	• Mobile sensing platform • Secure data delivery platform • Environment monitoring application
Mobile sensors	• **Weather sensors:** temperature, humidity, pressure, UV-A • **Movement sensors:** acceleration, geomagnetism, angular velocity • **Air sensors:** PM2.5 • **Location sensor**: GPS

2.3.1.2 Stakeholders engagement plan

The stakeholders of this pilot include garbage collection workers who are in charge of garbage collection, municipal officers who are responsible for environment monitoring, and citizens who consume the data for their own purposes. All of these stakeholders are the target users of this Secure Mobile Environment Sensing system over M-Sec platform in that they produce or consume environment data handled by the system. Regarding data production, the sensors are operated and capture data automatically while garbage collection is in progress. The garbage collection workers thus contribute to this pilot without being aware of it. In order to have contribution by municipal officers, KEIO will host meetings to show the effectiveness of the system. Citizens as participants will be recruited via M-Sec website assisted by Fujisawa local government for its advertisement. The following table shows a brief overview of stakeholders' engagement plan in this pilot.

Table 2-15: Use Case 3 Pilot 3.1 stakeholders and participants

Stakeholder: Garbage Collection Workers	KEIO asks ~10 workers for cooperation to this pilot study. The workers are currently in cooperation with KEIO for mobile environment sensing.
Stakeholder: Municipal Officers	KEIO asks ~2 officers in Fujisawa for cooperation to this pilot study. Fujisawa local government and KEIO are collaborating closely in Regional IoT consortium.
Participant: Citizens	50 citizens will be recruited via the M-Sec web page assisted by Fujisawa local government in advertising.

2.3.1.3 Data management plan

The following table shows a summary of the data management plan.

Table 2-16: Use Case 3 pilot 3.1 data management plan

Type of data	• Numeric data on environment information, such as temperature, humidity, PM2.5 density, etc. • Image data on environment information, such as road surface, graffiti, etc.
Format of data	• XML documents that encapsulate the aforementioned data
Data collection	• Over the course of the pilot, data will be generated from sensors, delivered through the data delivery platform and forwarded to applications in encrypted XML format via XMPP over TCP/IP.
Data storage	• Over the course of the pilot, data will be collected and entered into an SQL database
Data management	• All the data stored during the pilot will be kept for research purposes.
Data management principle	• Survey data will be generated only in an anonymised form. Therefore, the questionnaires, interview guidelines and other used instruments must not contain questions the answers of which could lead to the participant's identity – alone or in combination with other answers. • The anonymity and privacy of participants must be respected. Personal information must be kept confidential. Guarantees of confidentiality and anonymity given to the participants must be honoured, unless there are clear and overriding reasons to do otherwise. • In case that the participants must be registered at the M-Sec platform and the pilot clients, they must not be registered with their name. For example, an ID-code could be used instead. • The participants themselves have their data sovereignty. In the case the participant wants the deletion of their data, this has to be done without any undue delay. • The participant is allowed to change/ limit the access authorisation of their data collected at the M-Sec platform and the pilot clients. • Only information pertinent to piloting activities is permitted to be collected. • All researchers have the duty of confidence in regard to collected data. • The integrity of stored, processed and published data must be ensured by the researchers and the project consortium. • Data that are collected by the participant at the M-Sec platform must be treated with care.

- Participants must be informed that the data could be used for the project.
- Participants must be informed in which way the data could be used.
- The participants must be informed who has the data sovereignty.
- The participants must be informed when the collected data will be deleted.
- Appropriate measures must be taken by the researcher to protect the collected data.
- Appropriate measures must be taken by the researcher to store and process data in a secure manner.
- In case the participant withdraws from the pilot, the collected data at the platform must be deleted or the access to them must be impossible for others, without any undue delay.

2.3.1.4 Ethics plan

Participants, i.e. citizens in Fujisawa, are publicly recruited via the M-Sec website. Their role in this pilot is downloading/installing/using the application to refer to the environment data collected by the sensors. The following rule of this pilot will be explicitly announced to the participants.

- No privacy-related information is collected.
- Access logs are collected without any privacy information.
- The access logs will be used for research purposes only.
- Participants can uninstall the application at any time.

This information is provided on the M-Sec web site and the application's terms of use. Ethical approval will be granted by Keio University. All the data collected during this pilot will be stored in KEIO for 5 years after the end of the pilot as academic evidence of the study. After the 5 years, the data will be deleted.

2.3.1.5 Set up

A summary of this pilot set up is shown in the following table.

Table 2-17: Use Case 3 pilot 3.1 set up

Planning	• **Start Date:** M21 (March 2020) • **Duration:** M21 – M33 (12 months) • **Phases:** o **PHASE 1 – Collaboration set-up** (M21-M23): Pilot plan is explained to Municipal officers and garbage collection workers for further collaboration. o **PHASE 2 – MVP release** (M24-M26): Sensors installation & calibration. Connectivity tests. Front-end applications tests. Proof-of-Concept oriented. o **PHASE 3 – 1st Trial of the pilot** (M27): Integration with M-Sec platform. Iterative sub-releases. o **PHASE 4 –2nd Trial of the pilot** (M33): Iterative sub-releases. o **PHASE 5 – Pilot Evaluation** (M33-M36): All the logs (IDS, access, etc.) are analysed.

Pilot setup	• In this pilot, citizens and municipality representatives participating will be able to install in their devices an application featuring the visualisation of the current and the past environment information. • Municipal officers will be able to install a participatory sensing application in their devices. • Collected data are stored in a server operated by KEIO.
Evaluation methodology	• **KPI** o # port scans o # data sniffing o # breach attempts o # user authentications • **Surveys** o Two surveys to be conducted about satisfaction level - During 1st release - Final evaluation

2.4 Use Case 4: Secure and Trustworthy Hyper-connected Citizens Care

This section describes the pilot that will be carried out in the city of Fujisawa to validate Use Case 4.

2.4.1 Pilot 4.1

2.4.1.1 Definition

This pilot study probes the power of edge-side security mechanism for privacy protection by integrating a mobile sensing platform on a garbage collection vehicle (in operation for the last three years in Fujisawa city) and additional edge-side computing infrastructure.

More concretely, we develop a privacy-protected garbage counting system that can count the amount of garbage output in a per-house-hold basis, consolidate the garbage amount information in a city and visualise the analysis result towards citizens' and local communities' higher awareness for garbage amount and eventual better well-being in their daily lives.

Information related to personal identity will be secured so that it does not harm privacy. Garbage collection trucks use an onboard camera to count the number of garbage plastic bags thrown to the truck in each location. However, our edge-side computing infrastructure analyses such sensor data and modifies them into minimum data needed for this purpose (i.e. the count of the plastic bags) which do not harm privacy. Such privacy-protected computed data will be sent to the server side.

The heterogeneous system components involved in the data stream dissemination and the data streams on the communication link will be secured by the M-Sec platform.

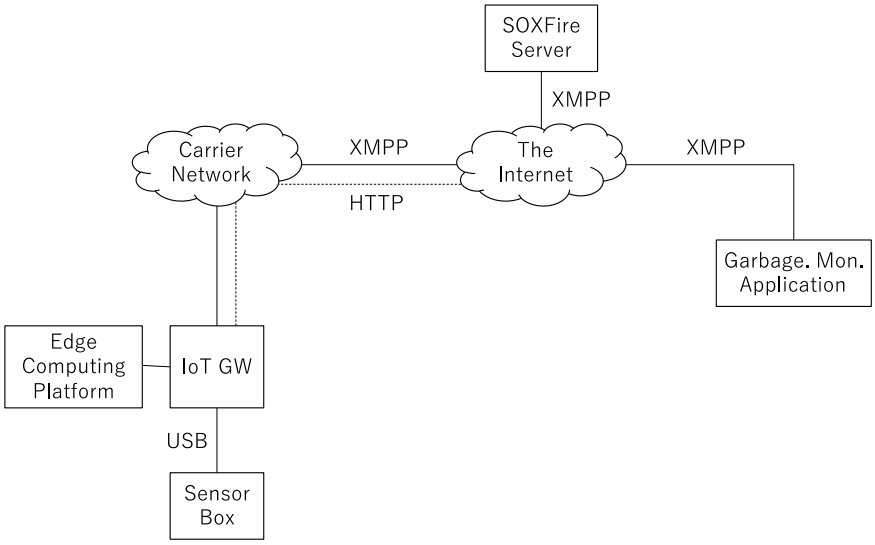

Figure 2—6: Topological overview of Use Case 4 Pilot 4.1

The pilot is planned to be held in Fujisawa city leveraging at least 10 garbage collection trucks that are part of the mobile sensing platform. It will last for 12 months during which we will evaluate the M-Sec platform and its technical components in terms of their effectiveness. The following table describes briefly the main aspects of the pilot execution.

Table 2-18: Use Case 4 pilot 4.1 definition

Pilot name	Privacy-secure Garbage Counting
Location of the pilot	Fujisawa City (Japan)
Infrastructure	• Mobile sensing platform • Edge computing platform • Data delivery platform • Garbage amount monitoring application
Mobile sensors	• **Camera sensor:** video image (view from the truck) • **Location sensor:** GPS

2.4.1.2 Stakeholders engagement plan

The stakeholders of this pilot include garbage collection workers who are in charge of garbage collection, municipal officers who are responsible for environment monitoring, and citizens who consume the data for their own purposes. All of these stakeholders are the target users of Privacy-secure Garbage Counting system in that they produce or consume environment data handled by the system. Regarding data production, the sensors are operated, capture data, and analyse the garbage count automatically while garbage collection is in progress. The garbage collection workers thus contribute to this pilot without being aware of it. In order to have contributions by municipal officers, KEIO will host meetings to show the effectiveness of the system. Citizens as participants will be recruited via M-Sec website assisted by Fujisawa local government for its advertisement.

The following table shows a brief overview of stakeholders engagement plan in this pilot.

Table 2-19: Use Case 4 pilot 4.1 stakeholders and participants

Stakeholder: Garbage Collection Workers	KEIO asks ~10 workers for cooperation to this pilot study. The workers are currently in cooperation with KEIO for mobile environment sensing.
Stakeholder: Municipal Officers	KEIO asks ~2 officers in Fujisawa for cooperation to this pilot study. Fujisawa local government and KEIO are collaborating closely in Regional IoT consortium.
Participant: Citizens	50 citizens will be recruited via M-Sec web page assisted by Fujisawa local government in advertisement.

2.4.1.3 Data management plan

The following table shows a summary of the data management plan.

Table 2-20: Use Case 4 pilot 4.1 data management plan

Type of data	• **Raw data from the sensors** • Garbage bag count (analysed from the raw sensor stream on the edge computing platform)
Format of data	• **Raw data format (Raw data from the sensors)** • Integer (Garbage bag count)
Data collection	• Over the course of the pilot, data will be generated from sensors and partially from the edge computing platform, and be delivered through the M-Sec platform and forwarded to applications.
Data storage	• Over the course of the pilot, data will be collected and entered into an SQL database
Data management	• All the data stored during the pilot will be kept for research purpose.
Data management principle	• Survey data will be generated only in an anonymised form. Therefore, the questionnaires, interview guidelines and other used instruments must not contain questions the answers of which could lead to the participant's identity – alone or in combination with other answers. • The anonymity and privacy of participants must be respected. Personal information must be kept confidential. Guarantees of confidentiality and anonymity given to the participants must be honoured, unless there are clear and overriding reasons to do otherwise. • In case that the participants must be registered at the M-Sec platform and the pilot clients, they must not be registered with their name. For

example, an ID-code could be used instead.

- The participants themselves have their data sovereignty. In the case the participant wants the deletion of their data, this has to be done without any undue delay.
- The participant is allowed to change/ limit the access authorisation of their data collected at the M-Sec platform and the pilot clients.
- Only information pertinent to piloting activities is permitted to be collected.
- All researchers have the duty of confidence in regard to collected data.
- The integrity of stored, processed and published data must be ensured by the researchers and the project consortium.
- Data that are collected by the participant at the M-Sec platform must be treated with care.
- Participants must be informed that the data could be used for the project.
- Participants must be informed in which way the data could be used.
- The participants must be informed who has the data sovereignty.
- The participants must be informed when the collected data will be deleted.
- Appropriate measures must be taken by the researcher to protect the collected data.
- Appropriate measures must be taken by the researcher to store and process data in a secure manner.
- In case the participant withdraws from the pilot, the collected data at the platform must be deleted or the access to them must be impossible for others, without any undue delay.

2.4.1.4 Ethics plan

Participants, i.e. citizens in Fujisawa, are publicly recruited via the M-Sec website. Their role in this pilot is downloading/installing/using the application to refer to the information (e.g, garbage bag) collected by the sensors. They are informed while the following are in effect:

- No privacy-related information is collected.
- Access logs are collected without any privacy information.
- The access logs will be used for research purposes only.
- Participants can uninstall the application at any time.

This information is provided on the M-Sec web site and the application's terms of use. Ethical approval will be granted by Keio University. All the data collected during this pilot will be stored in KEIO for 5 years after the end of the pilot as academic evidence of the study. After the 5 years, the data will be deleted.

2.4.1.5 Set up

A summary of this pilot set up is shown in the following table.

Table 2-21: Use Case 4 pilot 4.1 set up

Planning	• **Start Date:** M21 (March 2020) • **Duration:** M21 – M33 (12 months) • **Phases:** o **PHASE 1 – Collaboration set-up** (M21-M23): Pilot plan is explained to Municipal officers and garbage collection workers for further collaboration. o **PHASE 2 – MVP release** (M24-M26): Sensors installation & calibration. Connectivity tests. Front-end applications tests. Proof-of-Concept oriented. o **PHASE 3 – 1st Trial of the pilot** (M27): Integration with M-Sec platform. Iterative sub-releases. o **PHASE 4 – 2nd Trial of the pilot** (M33): Iterative sub-releases. o **PHASE 5 – Pilot Evaluation** (M33-M36): All the logs (IDS, access, etc.) are analysed.
Pilot Setup	• Garbage collection trucks are equipped with GPU-embedded computers that run the bag-counting algorithm. • Municipal officers are able to install an application, featuring visualisation of the amount of garbage collection, to their devices**.**
Evaluation methodology	• **KPI** o The number of privacy protections, i.e., the number of privacy-related objects filtered out from input images o The number of user authentications conducted for end-to-end security • **Surveys** o Two surveys to be conducted about satisfaction level - During 1st release - Final evaluation

2.4.2 Pilot 4.2

2.4.2.1 Definition

This pilot explores the possibility of secure sharing on citizen's affective information and information on the city, by using various types of technologies, such as mobile participatory sensing, edge-(mobile)-side computation for privacy protection, secure data sharing of sensed information.

More specifically, we develop a privacy-protected mobile participatory sensing platform in which citizens can sense and share information on their neighbourhood (city) with corresponding affective status information attached, and where such sensed information will be shared (1) securely among the citizen's community and (2) publicly with an appropriated privacy-protection mechanism.

The system overview and topology is illustrated in Figure 2—7. A smartphone application of this system will be distributed to citizens. When the citizens, during their daily lives, find notable happenings in the city (e.g. a crack on the road, a beautiful flower blooming, etc.) they take a photo of that by using the application. The application simultaneously captures the photo of the event and the user's face by using 2 cameras on the

smartphone simultaneously. Inside the application's "community" where appropriated admission/access control is implemented, the user can share the photos (both of the event and the user's face) with other community members.

On the other hand, for the local city's public data sharing area, the data with appropriate privacy protection processing will be shared so that no information on personal identity will be leaked to the public. The photo of the event along with the user's only affective status data (e.g., such as "smile degree" of the user's face) analysed from the user's facial expression will be shared. Those who are taking care of the local area, such as local city officers, view the posted publicly available photos along with the affective status of the photographer, and discuss possible actions towards better city conditions.

The heterogeneous system components involved in the data stream dissemination to the public data sharing area will be secured by the M-Sec platform.

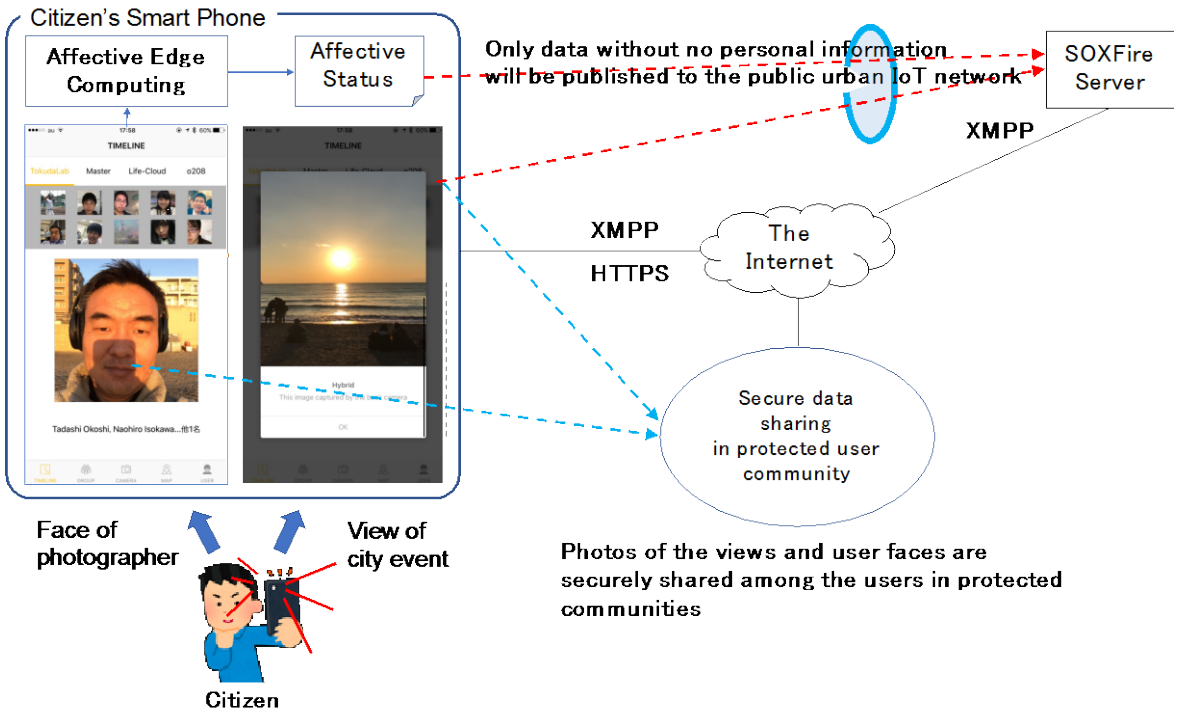

Figure 2—7: Overview of Use Case 4 Pilot 4.2

The pilot is planned to be held in Fujisawa city leveraging at least 30 users that are part of the mobile sensing platform. It will last 12 months during which we will evaluate the M-Sec platform and its technical components in terms of their effectiveness. The following table describes briefly the main aspects of the pilot execution.

Table 2-22: Use case 4 pilot 4.2 definition

Pilot name	Secure Affective Participatory Sensing of City Events
Location of the pilot	Fujisawa City (Japan)

Infrastructure	• Mobile participatory sensing platform • Edge affective computing platform • Data delivery platform • City event report application
Mobile sensors	• **Sensors on the smartphone** o Camera (in-cam, out-cam) o GPS o Light sensor o Gyroscope

2.4.2.2 Stakeholders engagement plan

The stakeholders of this pilot include local citizens who act as "participatory sensing" human sensors and municipal officers who are responsible for city planning discussion. In order to have contributions by municipal officers, KEIO will host meetings to show the effectiveness of the system. Citizens as participants will be recruited via M-Sec website assisted by Fujisawa local government for its advertisement. The following table shows a brief overview of stakeholders' engagement plan in this pilot.

Table 2-23: Use case 4 pilot 4.2 stakeholders and participants

Stakeholder: Municipal Officers	KEIO asks ~2 officers in Fujisawa for cooperation to this pilot study. Fujisawa local government and KEIO are collaborating closely in Regional IoT consortium.
Participant: Citizens	50 citizens will be recruited via M-Sec web page assisted by Fujisawa local government in advertisement.

2.4.2.3 Data management plan

Table 2-24: Use case 4 pilot 4.2 data management plan

Type of data	• **Raw data from the sensors** • Photographer's affective status data (estimated from the captured photo image)
Format of data	• **Raw data format (Raw data from the sensors)** • Array of double (Photographer's affective status)
Data collection	• Over the course of the pilot, data will be generated from the smartphone sensors and partially generated from the edge affective computing platform. Some parts of those data will be shared among the users of this system's community (with appropriated admission/access controls). Some other data will be delivered through M-Sec platform and shared publicly, after privacy-protection computing is applied on the

	smartphone.
Data storage	• Over the course of the pilot, data will be collected and entered into an SQL database
Data management	• All the data stored during the pilot will be kept for research purpose.
Data management principle	• Survey data will be generated only in an anonymised form. Therefore the questionnaires, interview guidelines and other used instruments must not contain questions, which answers could lead to the participant's identity – alone or in combination with other answers. • The anonymity and privacy of participants must be respected. Personal information must be kept confidential. Guarantees of confidentiality and anonymity given to the participants must be honoured, unless there are clear and overriding reasons to do otherwise. • In case that the participants must be registered at the M-Sec platform and the pilot clients, they must not be registered with their name. E.g. an ID-code will be applicable instead of it. • The participants themselves have their data sovereignty. In the case the participant wants the deletion of their data, this has to be done without any undue delay. • The participant is allowed to change/ limit the access authorization of their data collected at the M-Sec platform and the pilot clients. • Only information pertinent to piloting activities is permitted to be collected. • All researchers have the duty of confidence in regard to collected data. • The integrity of stored, processed and published data must be ensured by the researchers and the project consortium. • Data that are collected by the participant at the M-Sec platform must be treated with care. o Participants must be informed that the data could be used for the project. o Participants must be informed in which way the data could be used. o The participants must be informed who has the data sovereignty. o The participants must be informed when the collected data will be deleted. o Appropriate measures must be taken by the researcher to protect the collected data. o Appropriate measures must be taken by the researcher to store and process data in a secure manner. o In case the participant withdraws from the pilot, the collected data at the platform must be deleted or the access to them must be impossible for others, without any undue delay.

2.4.2.4 Ethics plan

The citizens' role in this pilot is downloading/installing/using the application of this system. They are informed while the following are in effect:

- No data related to personal identity will be uploaded to the public area.
- Access logs are collected without any privacy information.
- The access logs will be used for research purpose only.
- Participants can uninstall the application at any time.

This information is provided on the M-Sec web site and the application's terms of use. Ethical approval will be granted by Keio University. All the data collected during this pilot will be stored in KEIO for 5 years after the end of the pilot as the academic evidence of the study. After the 5 years, the data will be deleted.

2.4.2.5 Set up

A summary of this pilot set up is shown in the following table.

Table 2-25 : Use case 4 pilot 4.2 set up

Planning	• **Start Date:** M21 (March 2020) • **Duration:** M21 – M33 (12 months) • **Phases:** o **PHASE – 1 Collaboration set-up** (M21-M23): Pilot plan is explained to Municipal officers and citizen volunteers who are willing to evaluate this application. o **PHASE 2 – MVP release** (M24-M26): Sensors installation & calibration. Connectivity tests. Proof-of-Concept oriented. Basic usability test. o **PHASE 3 – 1st Trial of the pilot** (M27): Integration with M-Sec platform to public data publishing. Iterative sub-releases. o **PHASE 4 – 2nd Trial of the pilot** (M30): Iterative sub-releases. o **PHASE 5 – Pilot Evaluation** (M30-M33): Survey results and application logs are analysed.
Evaluation methodology	• **KPI** o The number of privacy protections, i.e., the number of privacy-related objects filtered out from input images o The number of user authentications conducted for end-to-end security • **Surveys** o Two surveys to be conducted about satisfaction level - During 1st release - Final evaluation

2.5 Use Case 5: A marketplace of IoT services for effective decision making

This section describes the pilot that will be carried out in both cities Santander and Fujisawa in order to validate cross-border use case 5.

2.5.1 Pilot 5.1

2.5.1.1 Definition

In this pilot, data collected through various methods (e.g. human data, environmental data, and industrial data) which are "buried" or not used by the society even though they could be valuable and sellable to organisations or people, will be distributed in a marketplace ensuring confidentiality, integrity, availability, and privacy of data following GDPR/PIPA regulations.

At first, we will set up a marketplace and accumulate data collected in other use cases from citizens, companies, organisations, as well as data automatically collected on the web and from IoT terminals, by applying the blockchain technology and multi-layer security measures.

The goal is exchanging data in a secure way, using blockchain in a marketplace between Santander and Fujisawa and implying gamification functionalities and rewarding mechanisms. The marketplace will be connected to various sensors so that live data streams and past data sets can be traded with virtual currencies. There will be data sets for free as well as in ordinary markets. Those can be traded on a common platform, allowing third parties to build diverse applications and services.

In the case of Santander, the municipality provides official and public data in exploitable formats (HTML, JSON, etc.) so they can reuse it for their own purposes, although, the main idea is to use it to develop new services or giving added value to the existing ones, through the Open Data Platform. This not only has an important economic potential, but also, gives advantage to transparency, participation and citizen collaboration, goals which are necessary in order to get a real open government.

The open data portal currently contains 90 open information pieces about Santander classified in different categories:

- **Transport:** urban public transports as buses (stops, timetables, lines, etc.), taxis (taxi-stops), bicycle (cycle-lane), parking and traffic information.
- **Urban planning and infrastructure:** including street-map, parks and gardens location, municipality buildings location, etc.
- **Shops:** stores location and shopping events.
- **Demography:** current and historic census.
- **Society and well-being:** news related to youth and participatory citizen.
- **Culture and leisure:** labour calendar, cultural programming.

Table 2-26: M-Sec Use Case5 Pilot 5.1 details

Pilot name	A marketplace of IoT services for effective decision making
Location of the pilot	Fujisawa City (Japan) , City of Santander (Spain),
Infrastructure	• IoT sensing devices • Secure data delivery platform • Smart City infrastructure

2.5.1.2 Stakeholders engagement plan

In this pilot, we will test the marketplace with a collaboration of citizens, shopkeepers and the municipal officers of Fujisawa city and City of Santander. By receiving the feedback and improving the marketplace, we will promote it and test it further with event organisers and companies that are interested into it.

2.5.1.3 Data management plan

The following table shows a summary of the data management plan.

Table 2-27: M-Sec Use Case 5 Pilot 5.1 data management plan

Type of data	• Raw data from other use cases, sensors, etc. • Metadata associated with raw data
Format of data	• Raw data formats
Data collection	• From other use cases • From citizens, companies, organisations • From web sites • From IoT terminals
Data storage	• Data will be collected and entered into an SQL database
Data management	• All the data generated during the pilot will be deleted. Before their elimination, the pilot evaluation report will generate anonymous and aggregated views of the data to illustrate the pilot actions and results aligned to the defined KPI's.
Data management principles	• The anonymity and privacy of participants must be respected. Personal information must be kept confidential. Guarantees of confidentiality and anonymity given to the participants must be honoured, unless there are clear and overriding reasons to do otherwise. • In case that the participants must be registered at the M-Sec platform and the pilot clients, they must not be registered with their name. E.g. an ID-code will be applicable instead of it.

- All researchers have the duty of confidence in regard to collected data.
- The integrity of stored, processed and published data must be ensured by the researchers and the project consortium.
- Data that are collected by the participant at the M-Sec platform must be treated with care.
- Participants must be informed that the data could be used for the project.
- Participants must be informed in which way the data could be used.
- The participants must be informed who has the data sovereignty.
- The participants must be informed when the collected data will be deleted.
- Appropriate measures must be taken by the researcher to protect the collected data.
- Appropriate measures must be taken by the researcher to store and process data in a secure manner.
- In case the participant withdraws from the pilot, the collected data at the platform must be deleted or the access to them must be impossible for others, without any undue delay.

2.5.1.4 Ethics plan

Participants, i.e., citizens in Fujisawa, and Santander are publicly recruited via the M-Sec website. Their role in this pilot is exchanging data in the marketplace collected by the sensors. They are informed with the following rules.

- No privacy-related information is collected.
- Access logs are collected without any privacy information.
- The access logs will be used for research purpose only.

This information is provided on the M-Sec web site and in the marketplace. Ethical approval will be granted and all the data collected during this pilot will be stored in the marketplace and after the end of the trial, the data will be deleted.

2.5.1.5 Set up

A summary of this pilot set up is shown in the following table.

Table 2-28: Use Case 5 pilot 5.1 set up

Planning	• **Start Date:** M15 (September 2019) • **Duration:** M15 – M33 (19 months) • **Phases:** o **PHASE 1 – Main features set-up** (M15-M17): Preparation of the agreed solution. o **PHASE 2 – Initial tests** (M18-M20): Initial version of the Marketplace.

	o **PHASE 3 – 1st Trial of the marketplace** (M21): Integration with M-Sec platform. Iterative sub-releases. o **PHASE 4 – 2nd Trial of the marketplace** (M30). Iterative sub-releases. o **PHASE 5 – Pilot Evaluation** (M31-M33). Questionnaires. KPIs follow-up report.
Evaluation methodology	• **KPI** o # smart objects including virtual sensors joining in the market place o # participants o # successful data exchanges • **Surveys** o Two surveys to be conducted about satisfaction level - During 1st release - Final evaluation

2.6 Use Case 6: Citizens as sensor

2.6.1 Pilot 6.1

2.6.1.1 Definition

The pilot related to this Use Case intends to create and implement the participatory environment in which citizens of Santander and Fujisawa provide their reports on various events, while sending also quantitative measurements of physical sensing provided by sensors that incorporate their cell phones. This way, citizens will feel more involved in the daily operations of their corresponding cities and municipal officers will get an additional information resource to help them carry out their jobs.

Thus, the goal consists in developing an application for the Smart City that allows the citizens to act as sensors, both by sending measurements collected by the sensors of their own mobile phones and by sending reports of events, good or bad, that seem newsworthy. These events will be accordingly checked and attended later by municipal personnel.

The users will be able to form a community attending to the interests that they manifest. In this way, they will be able to receive notifications when any other user reports something related to those interests.

This approach will be based on similar initiatives that were in use in both cities but that somehow were discontinued or did not include such kind of features, and will also integrate novelties such as the creation of gamification systems and delivery of prizes to the winners of such games, establishing competitions between both cities.

The implementation of a “like”/”commenting” system between users and/or local management staffs will also be considered, since this could be a motivation for the user to continue providing input. In addition, the

previous experiences suggest citizens are more inclined to report just bad news; the consortium will look for ways to encourage them to report also nice events.

In addition, and knowing that nowadays many people use social media to provide these reports, the solution will look for ways to let app users cross-post their reports directly on Twitter or Facebook. That way, this scenario will attract more people to the app.

Table 2-29: M-Sec Use Case 6 pilot 6.1 details

Pilot name	Citizen as sensor
Location of the pilot	Santander City (Spain), Fujisawa City (Japan)
Infrastructure	• Smart city infrastructure • MinaRepo application • Pace of the city legacy application

2.6.1.2 Stakeholders engagement plan

Engaging citizens of different ages portrays certain challenges. To do so, the consortium will exploit well-known mechanisms:

- Promotion through municipal communication channels.
- Meetings with different municipal services, such as neighbourhood associations.
- Involvement of youth municipal services.

2.6.1.3 Data management plan

The following table shows a summary of the data management plan.

Table 2-30: M-Sec Use Case 6 Pilot data management plan

Type of data	• Reports from real citizens: text, images • Measurements collected from sensors integrated in the user's mobile phone
Format of data	• Raw data format (Raw data from the sensors) • Plain text (reports) • Images
Data collection	• Over the course of the pilot, data will be generated from cell phones
Data storage	• Over the course of the pilot, data will be collected and entered into a SQL database
Data management	• All the data generated during the pilot will be deleted. Before their elimination, the pilot evaluation report will generate anonymous and aggregated views of the data to illustrate the pilot actions and results

	aligned to the defined KPIs.
Data management principles	• The anonymity and privacy of participants must be respected. Personal information must be kept confidential. Guarantees of confidentiality and anonymity given to the participants must be honoured, unless there are clear and overriding reasons to do otherwise. • In case that the participants must be registered at the M-Sec platform and the pilot clients, they must not be registered with their name. For example, an ID-code will be applicable instead. • All researchers have the duty of confidence in regard to collected data. • The integrity of stored, processed and published data must be ensured by the researchers and the project consortium. • Data that are collected by the participant at the M-Sec platform must be treated with care. o Participants must be informed that the data could be used for the project. o Participants must be informed in which way the data could be used. o The participants must be informed who has the data sovereignty. o The participants must be informed when the collected data will be deleted. o Appropriate measures must be taken by the researcher to protect the collected data. o Appropriate measures must be taken by the researcher to store and process data in a secure manner. o In case the participant withdraws from the pilot, the collected data at the platform must be deleted or the access to them must be impossible for others, without any undue delay.

2.6.1.4 Ethics plan

As this pilot is a cross-border pilot, discussion about the EU and Japan directive regarding privacy needs to be continued and reinforced with the experience of the first four pilots.

2.6.1.5 Set up

A summary of this pilot set up is shown in the following table.

Table 2-31: Use Case 6 Citizen as Sensor Pilot set up

Planning	• **Start Date:** M21 (March 2020) • **Duration:** M21 – M36 (15 months) • **Phases:** o **PHASE 1 – Main features set-up** (M15-M18): Preparation of the agreed solution. o **PHASE 2 – Initial tests** (M18-M21): Initial version of the app. o **PHASE 3 – 1st Trial of the pilot** (M21): Integration with M-Sec platform.

	Iterative sub-releases. o **PHASE 4 – 2nd Trial of the pilot** (M33): Iterative sub-releases. o **PHASE 5 – Pilot Evaluation** (M33-M36): Questionnaires. KPIs follow-up report.
Citizen as sensor data setup	• In this pilot, citizens and municipality representatives participating will be able to take part and lend a hand in the daily routines of their corresponding Municipalities through their active participation sending measurements and reports. • No actual action will be derived from the collection and analysis of presence data from detected devices. City of Santander and Fujisawa will be collecting the data but only for informational purposes.
Evaluation methodology	• **KPI** o # downloads o # registered users o # reports • **Surveys** o Two surveys to be conducted about satisfaction level - During 1st release - Final evaluation

3 Conclusions

This document provides the initial version of the M-Sec pilots that will be carried out in both pilot cities, Santander and Fujisawa, in order to validate uses cases defined in D2.1.

This validation will be carried out through 9 pilots (4 in Santander, 3 in Fujisawa and 2 cross-border pilots), proving thus project robustness, its high level of interoperability and, also, its ability to be compliant with GDPR regulation as far as it concerns the flow of data across different countries, the privacy and data protection measures that can be applied for the benefit of the citizen and data portability. A summary of these pilots is shown in the following table.

Table 3-1: Summary of M-Sec pilots

Pilot (s)	Names	City
Pilot 1.1	Reliable IoT environmental data devices with multi-layered security for a smart city	Santander
Pilot 1.2	Reliable IoT crowd counting data devices with multi-layered security for a smart city	Santander
Pilot 2.1	Home Activity Tele-assistance	Santander
Pilot 2.2	Social & Physical Wellbeing	Santander
Pilot 3.1	Secure Mobile Environment Sensing	Fujisawa
Pilot 4.1	Privacy-secure Garbage Counting	Fujisawa
Pilot 4.2	Secure Affective Participatory Sensing of City Events	Fujisawa
Pilot 5.1	A marketplace of IoT services for effective decision making	Fujisawa & Santander
Pilot 6.1	Citizen as sensor	Santander & Fujisawa

This initial version of M-Sec pilots includes a common approach, which has been adopted to homogenise the different pilots: each one of them includes a definition, a stakeholders' engagement plan, a data management plan, an ethics plan and, also, the setup description.

Finally, it is important to point out that as this is the first of three deliverables regarding pilots definition, setup and citizen involvement, therefore, any modification of the pilots will be included in the next deliverables D2.3 and D2.4.