Multi-layered Security Technologies

for hyper-connected smart cities

D2.3: M-Sec pilots definition, setup and citizen involvement report – first version

July 2020

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	D2.3.1 M-Sec pilots definition, setup and citizen involvement report – 1st version
Work Package	WP2
Submission date	July 2020
Deliverable lead	AYTOSAN/NTTE
Authors	TST, WLI, CEA, F6S, AYTOSAN, KEIO, NTTE, YNU
Internal reviewer	ICCS/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

#	Date	Authors (Organization)	Changes
v0.1	10 June 2020	Sonia Sotero (AYTOSAN)	Full ToC and initial content
v0.2	19 June 2020	Vanessa Clemente (WLI)	1st contribution on Pilot 2
v0.3	23 June 2020	Keiko Doguchi (NTTE)	1st contribution on Pilot 5
v0.4	30 June 2020	Akira Tsuge (KEIO)	1st contribution on Pilots 3 & 4
v0.5	30 June 2020	Arturo Medela (TST)	1st contribution on Pilot 1
v0.6	1 July 2020	Arturo Medela (TST), Akira Tsuge (KEIO)	Updated on Pilots 1 & 3
v0.7	3 July 2020	Arturo Medela (TST)	Updated on Pilots 1 & 2
v0.8	6 July2020	Vanessa Clemente (WLI), Keiko Doguchi (NTTE)	Updated on Pilot 2 & Pilot 5
v0.9	7 July 2020	Keiko Doguchi (NTTE), Sonia Sotero (AYTOSAN)	Updated on Pilot 5, Updated before July GA & Pilot 1
v0.10	9 July 2020	Sonia Sotero (AYTOSAN)	Updated on Pilot4&Pilot5
v0.11	10 July 2020	Arturo Medela (TST)	Updated on Pilot1
v0.12	10 July 2020	Keiko Doguchi (NTTE)	Updated on Pilot5
v0.13	13 July 2020	Vanessa Clemente (WLI)	Updated Pilot 2 and added some comments for other use cases to take into account
v0.14	14 July 2020	Sonia Sotero (AYTOSAN)	Stable version for internal review
v0.15	14 July 2020	Orfeas Voutyras (ICCS)	Internal review
v0.16	15 July 2020	Kenji Tei (WU)	Internal review
v0.17	15 July 2020	Mari Seki (NTTE), Sonia Sotero (AYTOSAN)	Updated on Pilot5, update before technical call
v0.18	15 July 2020	Arturo Medela (TST)	Updated on Pilot1
v0.19	16 July 2020	Keiko Doguchi(NTTE)	Updated on Pilot5
v0.20	16 July 2020	Sonia Sotero (AYTOSAN)	Updated on Pilot5
v0.21	17 July 2020	Jin Nakazawa, Akira Tsuge, Tadashi Okoshi (KEIO)	Updated on Pilots 3 and 4
v0.22	17 July 2020	Vanessa Clemente	Updated on Pilot 2
v0.23	17 July 2020	Sonia Sotero (AYTOSAN)	Version ready for internal review
v0.24	17 July 2020	Kenji Tei (WU)	Internal review
v0.25	17 July 2020	Orfeas Voutyras (ICCS)	Internal review
v0.26	17 July 2020	Sonia Sotero (AYTOSAN)	After internal review
v0.27	19 July 2020	Vanessa Clemente (WLI)	Internal review
v0.28	20 July 2020	Keiko Doguchi (NTTE)	Updated on Pilot 5
v0.29	20 July 2020	Jin Nakazawa (KEIO)	Updated on Pilot 3
v0.30	20 July 2020	Arturo Medela (TST)	Solved comments on Pilot 1
v0.31	21 July 2020	Keiko Doguchi (NTTE)	Modified a chart in Section 2
v0.32	21 July 2020	Tadashi Okoshi (Keio)	Updated on Pilot4
v0.33	21 July 2020	Keiko Doguchi (NTTE)	Merge Pilot4 section
v0.34	24 July 2020	Vanessa Clemente (WLI) Mathieu Gallissot (CEA)	Reviewed the deliverable Added 5V comments in UC1 and UC2
v0.35	29 July 2020	Tadashi Okoshi (KEIO)	Updated on Pilot 4
v0.36	29 July 2020	Keiko Doguchi (NTTE)	Updated on Pilot 5, Adopted review changes, Final

v0.37	30 July 2020	Vanessa Clemente (WLI)	Review deliverable and adapted format.
V0.38	31 July 2020	Tadashi Okoshi (KEIO)	Updated on Pilot 4
v1.0	31 July 2020	Vanessa Clemente (WLI), Keiko Doguchi (NTTE)	Version ready for submission

Table of Contents

List of Tables

List of Figures

Glossary

Acronym	Description	Acronym	Description
APPI	Act on the Protection of Personal Information	P	Pilot
D	Deliverable	PM25	Particulate Matter 2.5
DDoS	Denial of service	PR	Public Relations
DoA	Document of Action	QoL	Quality of Life
DPIA	Data Privacy Impact Assessment	QR code	Quick Response Code
GDPR	General Data Privacy Regulation	R	Result
GPS	Global Positioning System	SME	Small and medium-sized enterprises
HW	Hardware	SQL	Structured Query Language
ICT	Information and Communication Technology	T	Task
IoT	Internet of Things	TCP/IP	Transmission Control & Internet Protocols
JSON	JavaScript Object Notation	ToC	Table of Contents
KPI	Key Performance Indicator	UC	Use Case
MQTT	Message Queuing Telemetry Transport	UV-A	Ultraviolet A
Obj	Objective	VOC	Volatile Organic Compound
OS	Operating System	XML	Extensible Markup Language
XMPP	Extensible Messaging and Presence Protocol		

1 Introduction

1.1 Scope of the document

The deliverable 'D2.3 M-Sec pilots definition, setup and citizen involvement report – 1st version' provides a report on M-Sec pilots. The first approach of this deliverable was to provide a detailed report of the main outcomes of the pilots carried out in both pilot cities, Santander and Fujisawa, during the second year of the project. However, due to the unusual worldwide situation caused by the coronavirus in the last few months, the start of these pilots has been delayed and none of them has been able to begin by the date of this document's preparation.

Under these circumstances, we agreed to submit two versions of this deliverable: the current document, as the first version of D2.3, provides an extended detail on the pilots' initial plan, including among others, an update on data management plan, stakeholders' engagement plan, ethics plan and set up; while, the second version of this deliverable will be submitted once the first trial of the pilots is carried out, and will include the main results obtained, feedback captured and lessons learnt. This second version of D2.3 is planned to be submitted by November 2020 (M29).

The current deliverable takes into consideration feedback from the 1st year review. The document follows an iterative approach by submitting a new version at the end of the project, Deliverable 2.4, once the second trial of the pilots is completed and the results are analysed.

1.2 Relation to other WPs and Tasks

'Task 2.2 – M-Sec Pilots: Definition, setup and citizens involvement' receives input from the other WP2 tasks, in particular from 'Task 2.1 – Use cases description', where uses cases are described, 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, 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 has been defined. Finally, as it can be seen in the figure below, an iterative approach is followed which will enable that lessons learnt during the first trial of the pilots to be used as inputs for WP3 as well as 'WP4 – Multi-layered Security Technologies', and as a basis for improvements and updates of further developments, with the aim of providing an enhanced and more end-user-oriented solution during the second trial of the pilots.

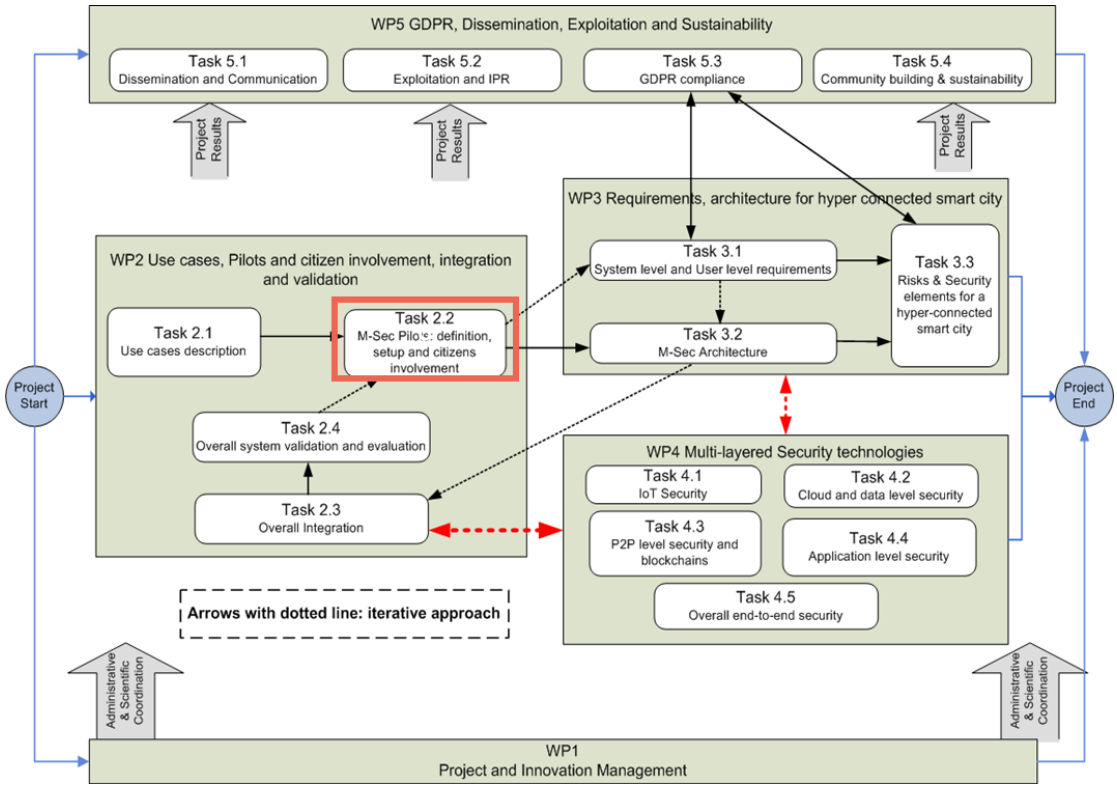

Figure 1—1: Relation of T2.2 to other WPs and Tasks

1.3 Methodology followed

The main objective of these pilots is to test and validate the M-Sec architecture and platform in real scenarios, ensuring that technological developments meet cities' needs and allowing M-Sec results to be exploited not only to develop but also to offer new smart city applications and services.

As stated above, the implementation of the M-Sec pilots follows an iterative approach, including two trials. During the first trial, in parallel with data collection and processing as well as service provision specific to each pilot, participants' feedback will be captured; and once this first trial is completed, the results obtained will be analysed, including the level of participation and the degree of satisfaction, while lessons learned will be identified. This useful information, which will be included in the second version of this deliverable, may be used as a basis for changes, improvements and updates for the further developments within WP3 and WP4. In this sense, it is important to note that during the definition of the pilots, stakeholders from both cities, Santander and Fujisawa, were contacted and their feedback was taken into account. Then, the second trial of the pilots will be carried out within the third year of the project, and, following a similar approach to the first trial, main outcomes and lessons learnt will be analysed and be included in the final version of M-Sec pilots' report, D2.4.

Furthermore, these pilots will contribute to delivering the key innovative results of M-Sec as well as ensuring the project meets its main objectives, in particular, those related to Objective 4 "Future decentralized IoT ecosystem." In this sense, the project has provided a set of Key Performance Indicators (KPIs), whose progress will be shown in 'D1.3 Project Progress Report', and which will enable M-Sec to measure its progress.

Last but not least, it is important to note that a successful pilot requires ensuring a balance between the needs of the different participants, including project stakeholders and end-users. Especially in the case of stakeholders (outside the consortium) and end-users, we need to attract their attention to take part in M-Sec pilots by providing them some incentives.

2 M-Sec pilots

This section provides a detailed description of the pilots that will be carried out in Santander and Fujisawa, in order to validate the use cases defined in D2.1 and update the plan described in D2.2.

The initial approach described in the previous deliverables included the definition of six use cases to be validated by the implementation of nine pilots, out of which four would be carried out in Santander and three in Fujisawa, while two cross-border pilots would be carried out in both pilot cities. Table 2-1 summarises these pilots.

Table 2-1: Initial approach of M-Sec pilots

Use cases	Pilots	Pilots' names	City
UC 1	Pilot1.1	Reliable IoT environmental data devices with multi-layered security for a smart city	Santander
	Pilot1.2	Reliable IoT crowd counting data devices with multi-layered security for a smart city	Santander
UC 2	Pilot2.1	Home Activity Tele-assistance	Santander
	Pilot2.2	Social & Physical Wellbeing	Santander
UC 3	Pilot3.1	Secure Mobile Environment Sensing	Fujisawa
UC 4	Pilot4.1	Privacy-secure Garbage Counting	Fujisawa
	Pilot4.2	Secure Affective Participatory Sensing of City Events	Fujisawa
UC 5	Pilot5.1	A marketplace of IoT services for effective decision making	Fujisawa & Santander
UC 6	Pilot6.1	Citizen as sensor	Santander & Fujisawa

During the second year of the project, the consortium has carried out a more thorough analysis of the use cases and related pilots, with the aim of identifying both possible synergies and the main distinguishing features, focusing on their contributions to the achievement of the project's objectives as well as the core M-Sec expected results. Table 2-2 summarises the results of this analysis. More information about M-Sec Objectives and Results can be found on the Description of Action (DoA), Section B1.1.2.

Table 2-2: Matching Use Cases & pilots with objectives & results

UCs/ Pilots	Obj 1.1	Obj 1.2	Obj 1.3	Obj 1.4	Obj 2.1	Obj 2.2	Obj 3.1	Obj 3.2	Obj 3.3	Obj 3.4	Obj 4.1	Obj 4.2	Obj 4.3	Obj 5.1	Obj 5.2	Obj 5.3	Res 1	Res 2	Res 3	Res 4
UC1																				
P1.1	yes	yes	yes	yes	no	yes	yes	yes	no	yes	no	yes	yes	yes	yes	no	yes	No	Yes	yes
P1.2	yes	yes	yes	yes	no	yes	yes	yes	no	yes	no	yes	yes	yes	yes	no	yes	No	Yes	yes
UC2																				
P2.1	yes	yes	yes	yes	no	yes	yes	yes	no	yes	no	yes	yes	yes	yes	no	yes	No	Yes	yes
UC3																				
P3.1	yes	yes	no	yes	no	yes	no	yes	no	yes	no	yes	yes	yes	yes	yes	yes	No	Yes	yes

UCs/ Pilots	Obj 1.1	Obj 1.2	Obj 1.3	Obj 1.4	Obj 2.1	Obj 2.2	Obj 3.1	Obj 3.2	Obj 3.3	Obj 3.4	Obj 4.1	Obj 4.2	Obj 4.3	Obj 5.1	Obj 5.2	Obj 5.3	Res 1	Res 2	Res 3	Res 4
UC4																				
P4.1	yes	yes	no	yes	no	no	yes	yes	no	yes	no	yes	yes	yes	yes	yes	yes	No	Yes	yes
P4.2	yes	yes	no	yes	no	yes	yes	yes	no	yes	no	yes	yes	yes	yes	yes	yes	No	Yes	yes
UC5																				
P5.1	yes	yes	no	yes	no	yes	yes	yes	no	yes	yes	no	yes	yes	yes	yes	yes	Yes	Yes	yes
UC6																				
P6.1	yes	yes	no	yes	no	yes	yes	yes	no	yes	no	yes	yes	yes	yes	yes	yes	No	Yes	yes

Taking into account that for some pilots both their relation to M-Sec objectives/results and their architectural view were similar, it was decided to merge some of the pilots and use cases. In particular:

- UC1, pilot1.1 and pilot1.2 are merged into a new pilot version, renamed as pilot1,
- UC2, pilot2.1 and pilot2.2 are merged into a new pilot version, renamed as pilot2,
- UC3, pilot3.1 and pilot4.1 are merged into a new pilot version, renamed as pilot3,
- UC4, pilot4.2 and pilot6.1 are merged into a new pilot version, renamed as pilot4,
- UC5, pilot5.1 remains as it is, and is renamed as pilot5.

While the number of use cases and pilots has been reduced, this fact does not imply a reduction in the workload or in the scope of the project, but rather a natural development based on the identification of common expected outcomes and the implementation of common solutions under an integrated M-Sec architecture.

The next table summarises the new version of the pilots to be implemented in the pilot cities.

Table 2-3: M-Sec pilots

Use cases	Pilots	Pilots' names	City
Use Case 1	Pilot 1	Secured IoT devices to enrich strolls across smart city parks	Santander
Use Case 2	Pilot 2	Home Monitoring Security System for ageing people	Santander
Use Case 3	Pilot 3	Secure and Trustworthy Mobile Sensing Platform	Fujisawa
Use Case 4	Pilot 4	Secure Affective Participatory Sensing of City Events (cross-border)	Fujisawa & Santander
Use Case 5	Pilot 5	Smart City Data Marketplace with secure Multi-layer Technologies	Fujisawa & Santander

Finally, considering the uniqueness of the different pilots and the need of homogenising them, a common approach similar to the one defined in D2.2 is adopted in the current report. Therefore, for each one of the pilots, the following specific information is provided:

- Synopsis, including a description of the pilot as well as an explanation of the new version of the pilot, when required.
- Stakeholders' identification, explaining how the main stakeholders are identified, which their interests are as well as what the particular benefits provided by M-Sec are.
- Recruitment criteria, including details such as the number of expected participants or technological capabilities, if required.
- Stakeholders' engagement plan: an update on the initial plan presented in D2.2, where stakeholders and end-users were identified, and how the recruitment would be carried out was explained.
- Data management plan: updating the initial plan detailed in D2.2, where the types and format of the data to be used as well as the methodology to be followed for their management were described.
- Ethics plan: providing an update on the initial plan explained in D2.2, which described how compliance with ethical issues had been ensured.
- Setup and timeframe: updating the initial planning.
- KPIs, including the metric indicators defined that will allow checking the success of each pilot.
- Questionnaires: as part of the evaluation methodology, surveys will be circulated among pilot's participants in order to get their feedback.
- Focus groups may be organised with pilot's participants to obtain detailed information about their participation in the pilot.
- Possible risks and corrective actions, trying to anticipate events such as getting a number of participants below the required minimum.
- User related threats, including those non –technical threats related to security threats identified in each pilot as well as the measures to overcome them thanks to M-Sec. This section complements the work done in 'D3.5 Risks and security elements for a hyperconnected smart city', where the detailed analysis of the main technical risks can be found.
- 5Vs definition of Big Data is followed in order to provide a standardized pilots overview in terms of:
    - Volume: Refers to the vast amounts of data generated every second.
    - Velocity: Refers to the speed at which new data are generated and the speed at which data move around.
    - Variety: Refers to the different types of data we can now use.
    - Veracity: Refers to the messiness or trustworthiness/quality/accuracy of the data.
    - Value: Refers to the extracted value of the data from a business or/and societal perspective.

  For each one of the pilots, firstly, it has been identified which 5V characteristics appear; then, the pilot's dimension has been scaled-up to force the appearance of the 5Vs, and finally, it is shown how the M-Sec solution would address them.
- What M-Sec is offering in terms of security, clarifying why pilots should adopt the M-Sec solution instead of other technologies.
- Finally, four core M-Sec expected results, indicating which pilot contributes most to which of the four key innovative results: Result1 "M-Sec distributed, robust and trusted platform", Result2 "M-Sec IoT Marketplace", Result3 "M-Sec smart city ecosystem" and Result4 "Revenue model and replication plan".

2.1 Pilot 1 (Use Case 1): Secured IoT devices to enrich strolls across smart city parks

This section describes the current status of the Pilot 1, which will be the translation into real-life of the ambitions sketched in Use Case 1.

2.1.1 Synopsis of the pilot

During the second year of M-Sec execution, taking into account the similar scope of the two different pilots initially proposed as part of UC1 and looking for a simplification of the message to send to potential users and stakeholders, the consortium decided to merge them both and present a single pilot to the world.

Hence, the main idea behind this pilot consists of deploying IoT devices that measure variables significant to the wellbeing of the city's inhabitants, such as noise or CO_2 levels, and overcrowding of selected areas through the sketching of heat maps. This information is relevant for the Municipality as well since it is not covered as of today as part of the smart city deployments already existing and this data would help when analysing the area and programming specific actions.

Users interested in taking part in the experience will find QR codes scattered throughout the pilot site (Las Llamas Park in Santander) for them to join the pilot.

A web application will enable these users to access and rate the quality of the data submitted, providing another layer of validation. Such activity will be encouraged via a rewards system targeting the most active users on the site.

Overall, the information provided by M-Sec will complement and enrich the one currently existing and will help the Municipality to extract valuable conclusions through the observation of diverse areas in the park. Figure 2–1 offers a view on one of the sections of this web application and how its structure helps to the enrichment of traditional information.

The main goals designed for the system that will be tested during the execution of this pilot will be:

- Enrichment of the current local information panels provided by the city government, through the introduction of digital sensors integrated in IoT devices and communications.
- Improvement of data security and integrity through the use of M-Sec layers in the different elements that compound the service. For instance, the IoT devices located in the lower layer will integrate hardware security features that will encrypt the data generated. Afterwards, looking up in the architecture, components such as the Companion database, along with the introduction of blockchain techniques, will help to prevent malicious attacks by a parallel encrypted system for data storage connected to the blockchain to ensure data tamper proof. A middleware between the IoT Devices and upper layers, Eclipse sensiNact, will help to provide a fine granularity access control mechanism to allow only authorised people to read (sensor measures) from the IoT devices.

Figure 2–1. Pilot 1 web application appearance

Table 2–4 summarizes the main details related to Pilot 1.

Table 2–4: Use Case 1 pilot 1 details

Pilot name	**Secured IoT devices to enrich strolls across smart city parks**
Location of the pilot	Santander City (Spain)
Users	Initial stage relies on users close to Santander partners in the Consortium before opening to citizens willing to participate. Acceptance and consent to participate in this pilot under the conditions expressed by the M-Sec consortium.
Infrastructure	IoT Devices with increased HW security. Web application front-end displaying enriched environmental and crowd data from IoT devices.
Sensors	IoT Environmental Monitoring devices integrate the following sensors: temperature, humidity, CO_2, VOC, and noise. Crowd counting IoT device: to estimate number of people in a specific sport.
Municipality Environmental Service	Dashboard: access to web app will enable establishing useful comparisons and preparing strategies.

2.1.2 Stakeholders' identification

The consortium has identified the stakeholders involved within this use case as well as their interest and particular benefits provided by M-Sec in order to establish the communication activities accordingly. Table 2–5 summarizes who they are and which their specific interests are.

Table 2–5: Use Case 1 pilot 1 stakeholder Identification

Stakeholder	Role	Interested in?	Specific benefits from M-Sec
Santander Municipality	IoT infrastructure providers	Carrying out new tests in its well-known city-wide living lab.	Enriching the urban laboratory dimension through the deployment of new devices, whose security has been reinforced.
Citizens	End users of the solution	Getting information on a simple way valid for them to know whether, for instance, it is the proper time to go to a certain spot or not.	Getting aggregated information of the park through a new user-friendly tool.
Municipal Services	Service providers	Establishing city-wide strategies depending on data retrieved from crowd devices and also act whenever environmental parameters value are unexpected	- Obtaining new reliable data sources, which can be used for internal consumption and/or be made available to citizens. - Establishing a new communication channel with citizens

2.1.3 Recruitment criteria

- In collaboration with the Municipal Environment Service, potential end-users have been identified, including nature lovers, by contacting environmentally-friendly associations, municipal staff, such as representatives from parks & gardens municipal service, and IT department, as well as, general public, by contacting neighbourhood associations.
- **Working status:** For the first trial of this pilot, a group of 10-15 "friend"-users from the groups identified above will be involved.
- **Minimum age of the participants:** 18 years old is the minimum required age to participate in the pilot.
- **Gender balance:** ideally 50% female and 50% male participants.
- **Technological capacities:** Since the web application has been designed to be user friendly, the only requirement could be to know how to handle a mobile phone or tablet.

2.1.4 Stakeholders' engagement plan

The consortium has created a plan for communication activities among stakeholders in order to achieve engagement and participation to validate M-Sec through Pilot 1. The plan followed is the one provided below in Table 2–6:

Table 2–6: Use Case 1 pilot 1 stakeholder recruitment actions

Recruitment Actions	Channel	Target User	Estimated Number of participants	When?	How?	How to keep users engaged?
Collaboration with Municipal Environmental Service	F2F meetings and online channels	Municipal Environmental Service	3	Since the beginning of the project	Regular meetings and conversations with Municipal Environmental Service representatives to identify potential end-users as well as to promote their participation	Taking into account their extensive knowledge of the park as well as the activities they organize, several meetings have been held to align municipal and project needs. They are actively participating in aspects such as the location of the devices, web appearance and content and identification of potential users.
Web promotion	Websites, Social Media Account	General public	~200	Summer 2020	Publish messages related to this Use Case and its pilot the moment the initial trial starts	Showing the usability of the proposed solution and the kind of enriched experience users will have. Secondly, by demonstrating how secure and robust is the solution provided.
Focus group	F2F meeting	General public	15-20	September2020	1-hour meeting to present the Use Case and its pilot to the public and show how the new tool works	Users will be engaged as long as they see that the solution offered does not require any complexity from their side in terms of installing devices or configuring them. Furthermore, partners will organize a follow-up meeting where users may share their experiences in order to improve the tool, as far as possible, for the next pilot phase.
Video promotion	Local channels	General public	5,000	October 2020	Brief Use Case 1 promotional video to play in local channels (info web channel, local buses closed loop)	Promoting periodic updates on the solution.

2.1.5 Data management plan

The strategy to deal with data generated in Pilot 1 will follow guidelines sketched in Table 2–7.

Table 2–7: Use Case 1 Pilot 1 data management

Type of data	• Raw data values from sensors (CO_2, noise level, number of attendees, etc.) • Metadata associated with raw data (network link strength, IoT device battery level, sensor type, etc.)
Format of data	• JSON data exchange format for transporting data & metadata within an MQTT channel.
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 topics will be created upon the different measurements collected by the IoT devices deployed in the park. • The corresponding back-end will subscribe to all these MQTT topics to properly present data in the web app.
Data storage	• Over the course of the pilot, data will be collected and entered into SQL database as JSON documents.

2.1.6 Ethics plan

The personal data which is collected at the registration phase of the "Park Guide" app enables the identification of a subject in a public space. However, it is not considered a high risk to privacy and, therefore, does not require a privacy impact assessment. This is due to the fact that the information requested during the registration process is just an e-mail address, to keep the user properly and directly informed of updates in the pilot, and a personal password. Upon consultation with Santander Municipality's data protection officer it was made clear this kind of information requested from users do not imply the need to conduct a DPIA.

During this registration stage, the user is first informed about the main concepts of the data protection, such as who the controller is, which the purpose of data collection is, what the legitimacy is, who the recipients are, as well as which their rights are; and then, they will authorize the data processing. Only when the user accepts this basic information, can they continue with the registration in the app.

Furthermore, data protection issues with handling of personal data will be addressed by the following strategies:

- Volunteers to be enrolled will be given comprehensive information, so that they are able to autonomously decide whether they consent to participate or not.
- The data gathered through logging, questionnaires, interviews and focus groups will be anonymised.
- Data will be stored only in anonymous form. The identifiers of the participants will be known only by the partners involved (TST) and will not even be exposed to the whole consortium.

More information about GDPR compliance of this use case can be found on D5.11 from Task 5.3.

2.1.7 Set up and Timeframe

Due to the impact of the COVID-19 pandemic, the pilot implementation needed to be postponed. The updated planning for the set up can be found in Table 2–8 below:

Table 2–8: Use Case1 Pilot 1 Steps assessment process and timeframe

Steps	What	Status	When
Step 1 Preparation	-GDPR compliance: - Evaluation of the need of DPIA - Assignment of roles (controller, processor) - Informed consent	As it can be found on deliverable D5.11, there is no need of DPIA. Roles have been defined, AYTOSAN and TS act as controller while the TST acts as Data Processor	M15-M22→ COMPLETED
Step 2 Recruitment	- Selected candidates	Identification of potential friend-users, starting with municipal staff and environmentally-friendly people	M19-M26→ NOT COMPLETED YET
Step 3 Training	-Training session to facilitate the use of the Park Guide web app	An online workshop will take place to show Park Guide functionalities	M26-M27→ NOT INITIATED YET
Step 4 Installation	- Sensors installation & calibration at Las Llamas Park	Strategy shared among involved partners and corresponding Municipality Services. Installation waiting until pandemic restrictions finish.	M26→ NOT INITIATED YET
Step 5 1st trial starts	-Initiation of the pilot	Pilot is expected to start in M27 (September 2020) for a total length of 3 months	M27-M29→ NOT INITIATED YET
Step 6 Initial measurement	-KPIs -Questionnaire	In order to get an initial feedback from end users, KPIs will be continuously monitored and a questionnaire will be sent 1 month after the initiation of the pilot. Results will be used to enhance the M-Sec components.	M27-M28→ NOT INITIATED YET
Step 7 Final assessment	-Questionnaire -Focus Group Discussion	A final questionnaire will be sent to finalize evaluation of the pilot. Additionally a focus group with users involved during the pilot will be conducted to collect further details.	M28-M29→ NOT INITIATED YET
Step 8 Data analysis	- Data reporting - Analysis of logging data - Synthesis of results and suggestions -Feedback to the Consortium	Evaluation results will be analysed and summarize to be transferred to technical partners for evaluation of further enhancements on their components.	M30→ NOT INITIATED YET
Step 9 Sub-iterative releases	-Enhancements and finalization of integration with M-Sec	The integration with M-Sec components will be completely finalized.	M30-M35

Steps	What	Status	When
Step 10 2nd Trial starts	-Initiation of the second phase of the pilot	Pilot is expected to start in M36 for a total length of 3 months	M36-M38→ NOT INITIATED YET
Step 11 Final assessment	-KPIs -Questionnaire	KPIs will be continuously monitored and a questionnaire will be sent after the pilot conclusion for the final evaluation.	M39→ NOT INITIATED YET

2.1.8 KPIs

To check the success of Pilot 1, a series of KPIs, listed in Table 2–9, will be monitored.

Table 2–9. Use Case 1 Pilot 1 KPIs

#KPI	Goal	How to measure?	Target	M-Sec Asset
#Participants	Minimum number of end users to test the solution provided	Number of end users registered into the system	≥50 users (1st trial: 10-15 friend users, 2nd trial: 50 participants)	Park Guide
#Active users	To evaluate the real activity of registered participants	Connections to the web app	≥20	Park Guide
#Data tampered	Verify data reliability (it has not been modified)	Use Blockchain, sensitive data from this use case can be tamper proof.	0	Companion Database and Quorum Blockchain
#Unauthorised intents to access to data	Avoid unauthorised users have access to sensitive data	Through smart contracts, it is possible to verify whether someone has authorization or not. Warning logs will be received to alert about it.	0	Companion DataBase + Quorum Blockchain
#DDoS attacks	Avoid attempts to disrupt normal traffic	Putting IoT devices on the Internet before going public and evaluating their interactions	0	IoTPOT
#Data Theft	Avoid infiltration in the overall M-Sec system and other project resources	Attacks to the IoT devices to get information (not available) and/or access to other elements in the system.	0	IoTVault

2.1.9 Questionnaires

For evaluation purposes, a survey will be conducted at the end of the initial piloting phase which will address topics related to usability, accessibility, scalability, reliability, integrity, accuracy and availability. Additionally, some open questions will be included in order to get new insights, ideas or enhancements raised by end users.

2.1.10 Focus groups

A focus group will be conducted at the beginning of the pilot experience involving Santander citizens and inviting other stakeholders as well. It will involve 10 to 15 people plus a moderator who will lead the exchange of ideas based on the brief presentation of the M-Sec project and its goals and the specific ambition of Pilot 1. A bunch of questions will be prepared for each participant to express their ideas and opinions. This will serve to provide relevant input into WP4 Multi Secure technologies for the second iteration of demonstrators.

2.1.11 Possible risks and corrective actions

- Number of participants:
  - Risk: The pilot does not acquire the desired number of participants.
  - Action: This pilot will be initially validated with 5 end users, considered people close to the partners involved in the experience. Soon later on, the recruitment of citizens will take place through different actions reaching the desired number of participants. Nevertheless, it may be possible that some people are reluctant to take part of an experimental action like this and/or any of them decide to voluntarily withdraw its participation for whatever reason (e.g. not useful data). In this case, the consortium will conduct another quick recruitment process to solve this situation.
- Technical problems:
  - Risk: Participants are frustrated when technical problems occur with the data provided by the IoT devices.
  - Action: The solution along with the integrated M-Sec components will be tested in detail before being tested by real users.
- Protection of personal data:
  - Risk: Leaks of personal data:
  - Action: The purpose of M-Sec is to avoid any malicious attack or breach of personal data. Therefore, M-Sec components integrated within the solution of Use Case 1 will provide extended security measures to avoid any risk related to it. Additionally, minimization principles have been applied in order to minimize the use of personal data only to what is strictly necessary for technical evaluation.

2.1.12 User Related Threats

The consortium has analysed the different risks for a solution like the one to be piloted on Use Case 1. Main technical risks can be found compiled in Deliverable 3.5 *"Risks and security elements for a hyperconnected smart city"*. Concerning the non-technical threats, they have been analysed within this deliverable and taken into account for commercialization's purposes. Hence, non –technical threats are summarized in the following Table 2–10:

Table 2–10: Use Case 1 pilot 1 user related threats

Type of User	Potential Threat (non-technical)	Related to a Security Threat	Measures to overcome the threat with M-Sec
Citizen	Incorrect treatment of personal data offered during registration process	Mishandling of personal data	• Park Guide
Citizen, Municipal Services	Erroneous information in the associated application that lead to incorrect decisions	Sensors are not providing reliable information (sensor connectivity, no data generated, etc.)	• EnMon, Crow, Park Guide
Citizen	What could happen if any malicious person puts false QR codes across the park?	Complaints to the pilot responsible. Bad PR for partners involved.	• Park Guide

2.1.13 5Vs definition of Big Data

Table 2–11 summarizes the baseline applied to Pilot 1 following the 5Vs definition of Big Data

Table 2–11 Use Case 1 Pilot 1 – 5Vs of Big Data

5Vs	Do the 5Vs appear in the Use Case/ demo? How?	Would the 5Vs appear in a scaled-up version of the UC? (exaggerated version)	How M-Sec will address/ addresses the 5Vs in the demos and the exaggerated scenario.
Volume	No, customized IoT devices like the ones developed within this Use Case may generate lots of data but no vast amounts of it (e.g. TeraBytes) depending on the desired application.	There are more than 500 National parks in Europe, covering an area of 5123,389 square kilometres, and over 30 in Japan, covering an area of 20,482 km^2. Knowing that Las Llamas park presents 11 hectares and the envisioned deployment will include 7 IoT devices, we can estimate that 340,000 devices could be required. If each one of them generates 3MB of data per day, we will be dealing with over 1TB of information per day.	Establish restrictive periods to not flood databases with not-so-useful data. This will also lead to a better battery usage. Use of sensiNact as aggregator / consolidator of data.
Velocity	No, the time of response from the sensors to	The required speed may be the same, but the actual speed reached will	The applications devised will not need to deliver this data

5Vs	Do the 5Vs appear in the Use Case/ demo? How?	Would the 5Vs appear in a scaled-up version of the UC? (exaggerated version)	How M-Sec will address/ addresses the 5Vs in the demos and the exaggerated scenario.
	integrate in the IoT devices is such that a lot of measurements could be delivered but no real time info is strictly required. . For instance, IoT devices in this pilot could send data every minute if needed.	depend on the capability of the infrastructure/system to handle the volumes of data.	in a high-speed manner.
Variety	No. Same type of structured data.	It could appear if more fields are added (e.g. type of park, types of exhibitions in parks, etc. giving an application like TripAdvisor).	---
Veracity	Yes, data could be tampered or even the own device could not transmit accurate data.	Depending on the sources.	Introduction of the secure element to prevent external attacks. Application of blockchain techniques in certain parts of the service to assure data veracity.
Value	Yes, risk analysis reports regarding the number of attacks avoided for instance using M-Sec capabilities and/or success of the service related to the engagement achieved with end-users.	Cities around the globe see as a great opportunity to take advantage of the deployment of this kind of solution, which may be especially relevant in a post-pandemic world. Interested stakeholders get data from these deployments and create services which may complement the ones already provided by cities, which in turn share their most relevant data with other cities experimenting similar situations.	Exploitation of data generated in Pilot 1 via M-Sec's IoT marketplace will provide a valid reference of the value associated to this information.

2.1.14 What M-Sec is offering in terms of security and Why Use Case 1 needs M-Sec?

This specific pilot needs the M-Sec privacy and security mechanisms due to the increasing number of attacks on IoT devices such as the ones that will be deployed in this experience. These attacks can go from the ones directed directly into the physical units, aiming at their integrity (external damages, power supply failures, even theft) to the ones affecting the data they generate and trying to get the personal information end users employ to interact with the system. Readers could refer to Deliverable 3.5 to get a wider view on the threats looming over these devices. There is a need to obtain reliable data from these IoT devices, since it will be required for Municipal services to implement effective strategies.

What M-Sec provides specifically is a collection of additional security measures from both a HW and an application standpoint, complemented by the introduction of blockchain techniques in this application field and the treatment of data in the Companion Database, to prevent external attacks that may lead to erroneous actions from end- users, understanding by this term not only citizens but also Municipal services. On the one hand, environmental sensing devices will provide useful and reliable information to establish much needed comparisons among environmental spots in the park physically separated (e.g. some of them closer to the road and others near the artificial lake) for end users to evaluate how healthy they are and municipality owners to act if pollution and/or noise goes above certain acceptable thresholds.

On the other hand, crowd counting devices will help authorities to keep track on whether attendees respect the social distancing imposed by the government rules looking to maintain people safe from virical impact, which is a topic more relevant than ever. Getting to know the number of people gathering at designated spots in the park and thanks to these devices being portable putting them on demand in other city areas will help to keep Santander safe.

2.1.15 Four Core M-Sec expected results

Table 2–12 shows how this pilot contributes to deliver the 4 key expected results, highlighting the one to which it contributes most.

Table 2–12 Pilot 1 – 4 Core M-Sec expected results

Use case/ Pilot	Title	Result1	Result2	Result3	Result4
Pilot1	Secured IoT devices to enrich strolls across smart city parks	**Yes**	No	Yes	Yes

This pilot contributes mainly to Result 1, *M-Sec distributed, robust and trusted platform*, by providing novel secured solutions to the IoT field already known in the Smart City context. In particular, talking about Santander, there have been several initiatives in the last few years with the Smart City as a primary focus, creating kind of a habit in the local and close stakeholders and in the overall population. What M-Sec provides is a much-needed update, assuring participants security, safety and reliability and, through Pilot 1, a way to exemplify it.

On the other hand, even though it does not directly contribute to Result2, *M-Sec IoT Marketplace*, it is true that data coming from this pilot is going to be integrated into the M-Sec marketplace.

Additionally, it contributes to Result3, *M-Sec smart city ecosystem*, by providing data complementary to the one already provided in the city of Santander via its Open Data Portal and thus attracting entrepreneurs and external developers that may find an opportunity to exploit them and develop their very own solutions for the Smart City.

Finally, it contributes to Result4, *Revenue model and replication plan*, via the development of IoT devices prototypes that may result highly relevant in the global context we find ourselves today. That is because keeping track of the people attending specific areas (e.g. Santander beaches) and/or events is now more

important than ever and thus event organizers and municipalities are in need of reliable solutions to get this information and act accordingly.

2.2 Pilot 2 (Use case 2): Home Monitoring Security System for ageing people

2.2.1 Synopsis of the pilot

Pilot 2 carried out in Santander city intends to face the main challenge of the rapid increase of elderly population during the past years caused by the increase of life expectancy due to medical, social and economic advances. Ageing people may feel isolated due to the lack of close family ties or the result of living alone. Additionally, many ageing citizens live with a constant fear of falling or becoming unwell without being detected or helped by others for a long time. Therefore, the consortium aims to provide a solution that already covers some issues related to wellbeing and safety at home.

This pilot is going to focus on home activity monitoring through the use of sensors such as presence sensors, bed occupancy sensors, window/door open sensors, and smart plugs. It has the aim to digitalise some of the current analogic-based, tele-assistance service provided by the Social Services department of the Santander City Council through a third-party operator.

Connected Care Assistance provides the following features:

- Connected Care Portal Platform user Management.
- Live Dashboard (alarms activated, latest activity)
- Patient/User Management (user data, device assignment, alarm assignment and custom setting, history data)
- Device Management (device info, connectivity & battery feedback)
- Alerts configuration (generic setting based on device/sensor type. Single Alert. Combined Alert)

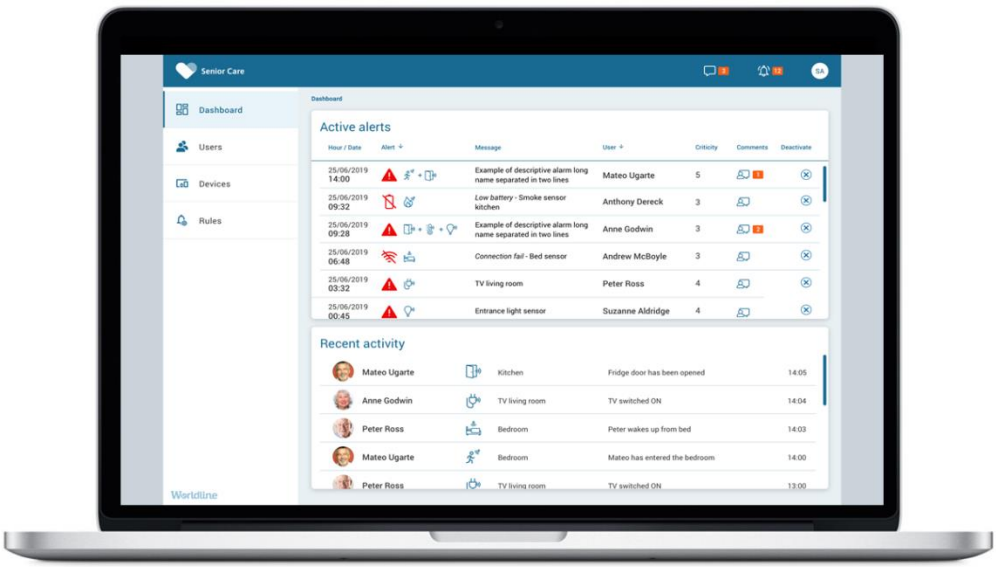

Figure 2—2: Connected Care Dashboard

The main goals designed for the system (Connected Care + M-Sec platform) that will be tested 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 such as the companion database with the quorum blockchain to prevent malicious attacks by a parallel encrypted system for data storage connected to the blockchain to ensure tamper-proof. A middleware between Connected Care and Home Sensor Devices, Eclipse sensiNact, which provides a fine granularity access control mechanism to allow only authorised people to read (sensor measures) or act on (actuators) IoT devices.

Table 2-13 describes the main aspects of the pilot execution.

Table 2-13: Use Case 2 Pilot 2 details

Pilot name	Home Monitoring Security System for Ageing People
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 home monitoring data from users
Home sensors	• **Connectivity Hub (Gateway):** to collect data from sensors (ZigBee) • **Motion sensor:** to detect human presence in a room • **Window/door open sensor:** to detect home doors/windows opening • **Bed Occupancy Sensor:** to detect if the user has left his/her bed and/or not returned after a specified period. • **Smart plug:** to detect activity in home appliances (e.g. TV)
Tele-service provider 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.

2.2.2 Stakeholders' identification

The consortium has identified the stakeholders involved within this use case as well as their interest and particular benefits provided by M-Sec in order to establish the communication activities accordingly.

Table 2-14: Use Case 2 Pilot 2 Stakeholder Identification

Stakeholder	Role	Interested in?	Specific benefits from M-Sec
Ageing People	End users of the solution	A solution that allows remote monitoring of their activity at home in order to live independently at his/her residence with all the security about that if something happens, someone from the tele assistance service will be notified. Due to the lack of technology knowledge, ageing people are interested on a usable solution that allows minimum technological contact. Additionally, end users expect a solution that protects their data vs malicious attacks.	M-Sec will enforce a trustworthy environment on the IoT ecosystem and facilitate and easier adoption by demonstrating how current potential risks of IoT can be mitigated by using M-Sec secure components. Furthermore, the solution provided, Connected Care, allows to remotely monitor users without complexity on the collection of data from end users point of view.
Caregivers	Closest network from end users of the solution	His/her relative can have a good QoL by being monitored through a secure and reliable system. Caregivers may want to be notified in case of an alarm generated.	M-Sec will provide the security and reliability on protecting the data processed from their relative in a secure way.
Tele-assistance providers	Monitor end users	Digitalize current analogic systems while at the same time monitor in a secure way all the users from the tele-assistance service.	Tele-assistance providers can benefit from the use of secure components from M-Sec to improve security on their IoT platforms.
AYTOSAN (In charge of the Teleassitance service)	To improve QoL of their citizens	Secure smart city solutions to increase QoL.	Deploy easily scalable technologies that bring tangible benefits (better services, reduced costs), but that at the same time include security and privacy mechanisms.
IoT Providers	Provider of Devices for home monitoring	First to increase sales by providing their devices at a higher scale (i.e if the UC is successful and replication occurs). Second, to increase security in their devices to differentiate from competitors, increase trustiness and become one of the main leaders on IoT device security.	To use potential outcomes from M-Sec to improve security from a device perspective.

2.2.3 Recruitment criteria

The minimum number of participants per Pilot 2 is 5. The main barrier to making the pilot open to a wider audience is the cost of the related Home IoT devices to be deployed at the user's home for monitoring purposes. However, for the preselection criteria, a higher number of users have been identified, 15 in total. Since this use case involves the recruitment of ageing people, health problems, surgeries, and others, may limit the availability of the participants during the pilot length and this must be considered.

- **Working status:** We focus on potentially isolated people therefore the participants are already retired under the following characteristics:
    - Persons who are currently getting the telecare service.
    - Persons who live alone
    - Persons who have not any disability or mental problem
    - Persons who have a network of relatives interested in joining the program.
    - Persons who are proactive in joining the pilot.
- **Minimum age of the participants:** 65 years people should be ideally between 65 and 80 years old.
- **Gender balance:** ideally 50% female and 50% male participants.
- **Technological capacities:** Since the installation of Home Sensor Devices will be performed by the Tele-assistance Provider at user's home it is not required good ICT knowledge. However, a balanced mix of participants including those with good ICT knowledge and those with poor ICT skills is desirable.

2.2.4 Stakeholders' engagement plan

The consortium has created a plan for communication activities among stakeholders in order to achieve engagement and participation to validate M-Sec through Pilot 2. The plan followed is the one provided below:

Table 2-15: Use Case 2 Pilot 2 stakeholder recruitment actions

Recruitment Actions	Channel	Target User	Estimated Number of participants	When?	How?	How to keep user engage?
Collaboration with municipal Social Services, and the current tele-assistance provider (Atenzia)	F2F meetings and online channels	Municipal Social Services and Atenzia	3	Since the beginning of the project	The Telecare service is a home assistance service via telephone, with immediate and permanent attention and an effective response to any incident or emergency situation. The City Council, specifically the Municipal Social Services, is in charge of the service, and it is provided through a service provider, Atenzia. Therefore, getting their involvement and collaboration has been essential in the development of the pilot.	From the beginning of the project and taking into account their extensive knowledge of the service and users, meetings have been held to align the municipal and project needs. They have been involved in aspects such as the choice of the devices to be deployed, the platform functionalities, the definition of alarms and privacy, with the aim of making the most of the pilot.
Conduct a training session to show to the tele-assistance operator the use of Connected Care as well as the benefits obtained through M-Sec.	Online	Tele-assistance Provider (Atenzia)	2-4	July 2020	The current tele-assistance operators use a platform for users and events management, therefore, they have good ICT knowledge. Atenzia has selected several of its operators to also use Connected Care platform, while continuing to offer the service committed to the city council.	On the one side by showing the usability of Connected Care vs the analogic current solution they have and the benefits obtained. Secondly, by demonstrating how secure and robust is the solution provided.

Recruitment Actions	Channel	Target User	Estimated Number of participants	When?	How?	How to keep user engage?
Pre-selection of a group of tele-assistance service users	Individual visits to each of the potential users at their residence.	Ageing People and Caregivers	15	February/ May 2020	The tele-assistance provider counts with over 2000 users who are already part of the monitoring service. From this network, a total of 15 users were pre-selected during the months of January and February taking advantage of the regular visits to their homes. Due to the COVID-19, in May it was necessary to confirm the availability of the pre-selected candidates.	During these individual visits, the pilot has been explained to each one of the 15 tele-assistance service users, taking into account his/her profile and circumstances, with the aim of assess his/her degree of interest in taking part of the pilot.
Confirmation of participants and installation of devices	Individual visits to each of the final users at their residence.	Ageing People and Caregivers	5	July 2020	Both Municipal Social Services and Atenzia recommend individual visits to each telecare user instead of group meetings, as well as minimizing the number of individual visits. Therefore, following their recommendations, during an individual visit to each one of the pre-selected candidates, he/she will be provided with a more detailed explanation of the pilot, given the informed consent to be signed and devices will be installed. For pilot purposes only 5 of the total 15 users will be finally selected to test the solution.	Users will be engaged as long as they see that the solution offered doesn't require any complexity from their side in terms of installing devices or configuring them.

2.2.5 Data management

Table 2-16: Use Case 2 Pilot 2 data management

Type of data	• Raw data values from sensors (movement, occupancy, voltage, frequency, ON/OFF values, 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.

2.2.6 Ethics plan

This pilot implies the processing of personal data from 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 have conducted an evaluation of the need to conduct a Data Privacy Impact Assessment (DPIA) as defined by the GDPR.

The consortium has based the criteria evaluation of the need of DPIA under GDPR (General Data Protection Regulation), Article 35 that sets out three types of processing, which always requires conducting a DPIA[1]. Furthermore, we analysed the Treatment list of DPIA[2] with eleven (11) criteria to be considered.

During the assessment, any criteria were considered as applicable to the current use case.

The pilot will be tested within a small group of individuals, in total 5 end users, mainly because of the limited number of IoT home sensors packs that the consortium can provide within budget. These users are above 65 years old but in any case, they are independent ageing people.

In no case, the participant of the pilot will be prevented from exercising his right or access to a good or service. In the informed consent (that can be found within Deliverable D5.11 GDPR), it will be stated that

[1] https://gdpr.eu/article-35-impact-assessment/
[2] https://www.aepd.es/sites/default/files/2019-09/listas-dpia-en-35-4.pdf

participation is voluntary and at any time the user can exercise the right to leave without causing any kind of impact on the contracted service that he/she has with the tele-assistance company.

Furthermore, the use case validates the technology developed on M-Sec, applying multiple security mechanisms on different layers, however the use of new technologies doesn't involve new forms of data collection and use with risk for the rights and freedoms of people. It only provides an enhancement on the security aspect.

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

- Only the data necessary for the conduct of the experiment will be collected. Minimization controls have been applied only to process personal data that is considered essential for conducting the pilot. Therefore, the consortium will only collect data that is necessary for validating the project's impact and improving the development of the technology.
- The solution includes the integration of several secure components developed or enhanced by M-Sec to provide additional secure mechanisms and ensure personal data protection.
- A strict application of the principles of accountability and transparency to users will be adopted.

Furthermore, data protection issues with handling of personal data will be addressed by the following strategies:

- Volunteers to be enrolled will be given comprehensive information, so that they are able to autonomously decide whether they consent to participate or not.
- An informed consent will be provided showing the purposes of the research, the procedures, potential inconvenience or benefits as well as the handling of their data (protection, storage) will be explained (available on D5.11 GDPR).
- In order to make the research transparent, participants will sign this consent form before taking part in the pilots.
- The data gathered through logging, questionnaires, interviews and focus groups will be anonymised.
- Data will be stored only in an anonymous form so that identifiers of the participants will only be known by the partners involved (AYTOSAN and WLI) and will not even be exposed to the whole consortium.

More information about GDPR compliance of this use case, it can be found on D5.11 GDPR.

2.2.7 Set up & Timeframe

- 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 containing 4 types of sensors (bed occupancy sensor, door/window open sensor, motion sensor and smart plug). They will all contain a gateway hub for sensor connectivity.
- The Tele-assistance company and care giving network will be provided with a web front-end displaying enriched monitoring & emergency data from users.

Due to Covid-19, the pilot implementation has been postponed. The updated planning for the set up can be found below:

Table 2-17: Use Case2 Pilot 2 Steps assessment process and timeframe

Steps	What	Status	When
Step 1: Preparation	-GDPR compliance: Conducted a compliance assessment of Data protection Evaluation of the need of DPIA Assignment of roles (controller, processor) Joint controller agreement and Data Processing Agreement Informed Consent	As it can be found on deliverable D5.11, there is no need of DPIA. Roles have been defined, AYTOSAN and WLI act as controller while the teleassistance provider acts as Data Processor A joint controller agreement between WLI and AYTOSAN, as well as a Data Processing Agreement between AYTOSAN and ATENZIA will be signed before the installation of the different devices. An informed consent templated for this use case has been included within D5.11.	M15-M21→ COMPLETED
Step 2 MPV ready	- Connected Care ready and integrated with applicable M-Sec secure components	Connected Care has been customized for the purpose of the use case and integrated with some of the M-Sec available components (Companion DataBase, Quorum Blockchain, Eclipse Sensinact and IoT MarketPlace).	M15-M25→ COMPLETED
Step 3 Recruitment	- Selected candidates	Several Meetings with Social Services and tele-assistance provider have been conducted to agree on the user's selection requirements. From a total of 15 preselected candidates, 5 have been finally selected.	M19-M25→ COMPLETED
Step 4 Training	- Training session to facilitate IoT home sensors installation and the use of the Connected Care	An online workshop of two hours has taken place to show Connected Care functionalities as well as devices installation procedure	M25→ COMPLETED
Step 5 Installation and configuration	- Sensors installation & calibration at user's home - Distribution and signature of the informed consent	Specific employees from the tele-assistance provider have successfully installed and configured the devices Informed consents have been distributed accordingly and signed by the participants	M25→ COMPLETED
Step 6 1st trial starts	-Initiation of the pilot	Pilot is expected to start in M26 (August 2020) for a total length of 3 months	M26-M28→ NOT INITIATED YET
Step 7 Initial	-KPIs	In order to get an initial feedback from end users,	M26-M27→

Steps	What	Status	When
measurement	-Questionnaire (ageing people and tele-assistance provider)	KPIs will be continuously monitored and a questionnaire will be sent 1 month after the initiation of the pilot. Results will be used to enhance the M-Sec components.	NOT INITIATED YET
Step 8 Final assessment	-Questionnaire (ageing people and tele-assistance provider) -Focus Group Discussion (tele-assistance provider)	A final questionnaire will be sent to finalize evaluation of the pilot. Additionally a focus group with users from the tele-assistance provider involved during the pilot will be conducted to collect further details.	M28-M29→ NOT INITIATED YET
Step 9 Data analysis	- Data reporting - Analysis of logging data - Synthesis of results and suggestions -Feedback to the Consortium	Evaluation results will be analysed and summarize to be transferred to technical partners for evaluation of further enhancements on their components.	M30→ NOT INITIATED YET
Step 10 Sub-iterative releases	-Enhancements and finalization of integration with M-Sec	The integration with M-Sec components will be completely finalized.	M30-M35
Step 11 2nd Trial starts	-Initiation of the second phase of the pilot	Pilot is expected to start in M36 for a total length of 3 months	M36-M38→ NOT INITIATED YET
Step 12 Final assessment	-KPIs -Questionnaire (ageing people and tele-assistance provider)	KPIs will be continuously monitored and a questionnaire will be sent after the pilot conclusion for the final evaluation.	M39→ NOT INITIATED YET

2.2.8 KPIs

To achieve success, KPIs are defined through metric indicators. The idea is to focus on the domains, areas, fields and critical factors, and to address the elements that are needed to complete the evaluation and identification of results to assess design, validation and testing of the M-Sec framework in terms of security provided.

Table 2-18: Use Case2 Pilot 2 KPIs

#KPI	Goal	How to measure?	Target	M-Sec Asset
#Participants	Minimum number of end users to test the solution provided.	Number of end users (ageing people) registered into the system	≥5 users	Connected Care

#KPI	Goal	How to measure?	Target	M-Sec Asset
#Daily Home Activity Data	To evaluate the volume of data generated and its scalability.	Raw data sent from the Home IoT sensors to Connected Care	TBD (applicable for a second pilot phase)	Connected Care
#Data frequency	To evaluate speed at which new data is generated	Latency time	≤25s	Connected Care
#Events that have been handled during the length of the pilot	To evaluate the number of events raised and their reliability	Number of alarms that have been addressed	≥ 60 (4 alarms/month per user)	Connected Care
#Data tampered	Verify data has not been modified	Thanks to Blockchain, sensitive data from this use case can be tamper proof due a hash pointer. The hash will indicate whether data has been modified. Worldline as owner of the solution provided to this use case, will try to modify data to check the vulnerability of the system and the validation of the hash function.	3 Attempts / 3 Detections	Crypto companion DataBase and Quorum Blockchain
#Unauthorised intents to access to data	Avoid unauthorised users have access to sensitive data	Through smart contracts, it is possible to verify whether someone has authorization or not. Warning logs will be received to alert about it.	3 Attempts / 3 Detections	Crypto Companion DataBase + Quorum Blockchain
#Data exchanged	To evaluate the business value of the anonymized data sent from Connected Care to the M-Sec Marketplace	Transactions handled in the Marketplace. Data are sent every 24h per dataset. Since there are 4 types of home sensor, there will be 4 datasets/day. Total pilot length: 360	>4 (1st Pilot Phase) >20 (2nd Pilot Phase)	MarketPlace
#false positive events	Verify the reliability of the sensors	Manual way by verifying the reliability of the data with the end user	<5	Connected Care
#End points accessed	Higher number of end points higher vulnerability grade	Access log file	<10	Whole Pilot System

2.2.9 Questionnaires

For evaluation purposes, two surveys will be sent to the two types of end-users (ageing people and tele-assistance provider). Questions will be related to usability, accessibility, scalability, reliability, integrity, accuracy, and availability. Additionally, some open questions will be conducted in order to get new insights, ideas, or enhancements raised by end-users.

2.2.10 Focus Group

A focus group will be conducted at the end of the trial with the tele-assistance provider. It will involve 5 to 10 people plus a moderator who will lead the exchange of ideas based on 10-15 questions where the main purpose will be that each participant expresses their ideas and opinions. This will serve to provide relevant input into WP4 Multi Secure technologies for the second iteration of demonstrators.

2.2.11 Possible risks and corrective actions

- Number of participants:
  - Risk: The pilot does not acquire the agreed number of participants.
  - Action: This pilot will be validated with 5 end users. However, it may be possible that any of the selected end users decide to voluntarily withdraw its participation for some reason (health, not feeling attracted, etc.). In this case, the consortium has preselected 10 additional users to cover a participant from the pilot eventually.
- Time and effort for involvement of test-users:
  - Risk: Participants do not have enough time to participate in testing the connection
  - Action: End users will not have to perform any action from their side to validate the solution. Devices will be installed and configure by the Tele assistance provider, supported by WLI. The webapp provided to access to the data collected from home sensors is just provided as optional for the end-users. There is not a need to access the webapp since all the alerts will be monitored by the third party providing the service of tele- assistance.
- Technical problems:
  - Risk: Participants (end-users and tele-assistance provider) are frustrated when technical problems occur with the prototypes.
  - Action: The solution, along with the integrated M-Sec components, will be tested in detail before being tested by older people and the service provider.
    Additionally, we will provide a bug tracking system where the tele-assistance party can report about problems with the system. Finally, other communication channels, such as telephone and email, will be provided in order to expedite the resolution of technical problems.
- Protection of personal data:
  - Risk: Leaks of personal data:
  - Action: The purpose of M-Sec is to avoid any malicious attacks or breach of personal data. Therefore, M-Sec components integrated within the solution of UC2 will provide extended

security measures to avoid any risk related to it. Additionally, minimization principles have been applied in order to minimize the use of personal data only to what is strictly necessary for the technical evaluation.

2.2.12 User Related Threats

The consortium has analysed the different risks for a solution like the one to be piloted on Use Case 2. Main technical risks can be found within D3.5 Risks and security elements for a hyperconnected smart city. Concerning the non-technical threats, they have been analysed within this deliverable and taken into account for commercialization's purposes. Non –technical threats are showed in Table 2-19:

Table 2-19: Use Case 2 Pilot 2 User related threats

Type of User	Potential Threat (non-technical)	Related to a Security Threat	Measures to overcome the threat with M-Sec
Ageing People	Lack of trust on the monitoring system (afraid of not being detected by the system)	Sensors are not providing reliable information (sensor connectivity, no data generated, false battery status, tamper data, etc.)	• Evaluation of the number of false positive alarms. • Security in terms of data tamper proof and authorization mechanisms have been integrated with the solution
Ageing People	Low perceived value. Not willing to pay for a service such as tele-assistance monitoring	Security components developed on M-Sec are not as promising as it was established due to immature technology Difficulty on showing in a materialized way security benefits	• Workshops to create awareness about importance on data protection. • Internal lab tests from the components developed
Tele Assistance Provider	Resistance of moving from analogical to digital solution	Security components may not work properly. Difficulty on showing benefits since it is not a visible solution. Bugs appear during the pilot validation making the solution unstable to be accepted.	• Workshops to create awareness about importance on data protection and benefits from M-Sec • Internal lab tests from the components developed
IoT Provider	IoT device vendors lack incentives to enhance security	Not valuable value perceived in terms of security at the IoT device and Gateway level	• Workshops to estimulate adoption of M-Sec components and show the competitive advantage on providing extended security

2.2.13 5Vs definition of Big Data

The volume of data is rapidly growing. This data explosion is a reality that businesses must both face and exploit in a structured and aggressive way to create value for itself and its customers and in all sectors. One popular framework or approach that has been useful to address the technical and managerial aspects of Big Data, including emerging issues, challenges, promises, and opportunities is the 5Vs framework. On the following table, the consortium provides how the 5Vs appears on UC2 and how M-Sec will address them.

Table 2-20: Use Case2 Pilot 2 5Vs of Big Data

5Vs	Do the 5Vs appear in the Use Case? (current pilot)	Would the 5Vs appear in a scaled-up version of the UC? (exaggerated version)	How M-Sec will address/ addresses the 5Vs in the current pilot scenario and the exaggerated scenario.
Volume	Yes, specific home sensor devices can generate large datasets of data like for example the Smart Plug that it is continuously monitoring the voltage and the AC frequency. - High activity: 1 reading (100 bytes) every 5 minutes -> 0.3 bytes / s - Low activity: 1 reading every 30 min -> 0.001 byte / s	The number of seniors in EU and Japan (>65 years old) are estimated to be 183 million. Therefore, the estimated data amount per house per day, supposing that the average number of member is 1.5 would be: -High activity: 25 million readings (25,000,000 bytes) every 5 minutes→ 83,333 bytes/s	Use of sensiNact as an aggregator of data with capabilities to consolidate these data.
Velocity	Yes, depending of the number of users, vast amounts of data can be generated, collected and analyzed. -Latency Time:20s	The required speed may be the same, but the actual speed reached will depend on the capability of the infrastructure/system to handle the volumes of data.	Use of sensiNact as an aggregator of data with capabilities to consolidate these data.
Variety	No. Same type of structured data.	No. Same type of structured data	NA
Veracity	Yes, data could be tampered or even the own device could not transmit accurate data.	Yes, data could be tampered or even the own device could not transmit accurate data.	Hash created by Blockchain and stored in the encrypted Companion DataBase
Value	Since this pilot involves the participation of only 5 users, aggregated data would not be considered useful for consultation.	Yes, risk analysis reports regarding the number of attacks avoided for instance using M-Sec capabilities / anonymized data of users of the system regarding their habits (by age, by type of sensor, etc.)	Connected Care Assistance along with M-Sec MarketPlace

2.2.14 What M-Sec is offering in terms of security and Why Use Case 2 needs M-Sec?

There are a lot of benefits of using the M-Sec platform, the security of the Connected Care application can be improved in all layers. By using M-Sec, it is possible to go beyond compliance with GDPR by adding additional security measures to prevent external attacks that may lead to erroneous actions from end-users.

One of the benefits is high level of security that provides the use of the quorum blockchain. Blockchain is designed relying on digital signatures and encryption increments the level of data security, not allowing tampering because the data stored in a Blockchain is immutable. It also reduces the thread of been hacked, as the information is distributed among all nodes in the network.

Another asset that increases the security for sensitive data is the companion database that together with the blockchain, gives the possibility to get compliant with the GDPR. Blockchain does not allow the modification or deletion of data, so if some user wants to delete personal information cannot do it. The companion database allows to have sensitive data stored in an encrypted database linked with a hash saved in a blockchain's transaction.

Furthermore, by using sensiNact, Connected Care provides a fine granularity access control mechanism to allow only authorized people to read raw data or interact with IoT devices.

2.2.15 Four Core M-Sec expected results

Table 2–21 shows how this pilot contributes to deliver the 4 key expected results, highlighting the one to which it contributes most.

Table 2–21 Pilot 2 – 4 Core M-Sec expected results

Use case/ Pilot	Title	Result1	Result2	Result3	Result4
Pilot2	Home Monitoring Security System for ageing people	Yes	No	Yes	**Yes**

This pilot contributes mainly to Result 4 from the project which corresponds to *'Revenue model and replication plan'*. The solution proposed, as explained above, it pretends to serve as a tool to reduce loneliness on ageing people while at the same time preserving their wellness. The remarkable improvements in medical, social and economic are the main driver of the increase in the life expectancy over the past century. Additionally, the current situation the population is facing around Covid-19, has contributed to create a higher interest from stakeholders on monitoring solutions. For example, if additionally to home sensors, health sensors were added, Connected Care assistance would allow to monitor in a safe way, users who are infected with immediate detection of worsening conditions and reducing the saturation of hospitals and health centers. Furthermore, it is of special relevance to highlight that these kinds of solutions often process a lot of sensitive data. Thanks to M-Sec, end to end security can be demonstrated, protecting the system from malicious attacks. In comparison with other solutions in the market, pilot 2 value added in terms of security will generate trustiness around the system. On the one side, ageing people will be more

confident on teleassistance services, attracted mainly due to the preservation of their data and reliability in the system. On the other side, companies will feel attracted to replicate our solution on top of M-Sec due to the end-to-end approach offered as well as the reliability and robustness of the system.

Although, it does not directly contribute to Result2 *'M-Sec IoT Marketplace'*, it is true that data coming from this pilot is going to be integrated into the M-Sec marketplace in an anonymised way. Data sent to the marketplace will be mainly raw data collected from home sensors. Personal information from the user, including for instance ID from the sensor or location will not be transferred.

Additionally, it contributes to Result1 *'M-Sec distributed, robust and trusted platform'* by integrating several M-Sec core system components to increase end-to-end security (Crypto Companion DataBase, Eclipse sensiNact, M-Sec blockchain). ….

Finally, it contributes to Result3, *'M-Sec smart city ecosystem,* by involving several stakeholders (i.e. IoT providers, service providers) around the solution and the potential offering of M-Sec as well as the benefits obtained.

2.3 Pilot 3 (Use case 3): Secure and Trustworthy Mobile Sensing Platform

2.3.1 Synopsis of the pilot

Pilot 3 carried out in Fujisawa city intends to face the main challenge of the environment data shared among stakeholders with trust. 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 WP4. 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 WP4.

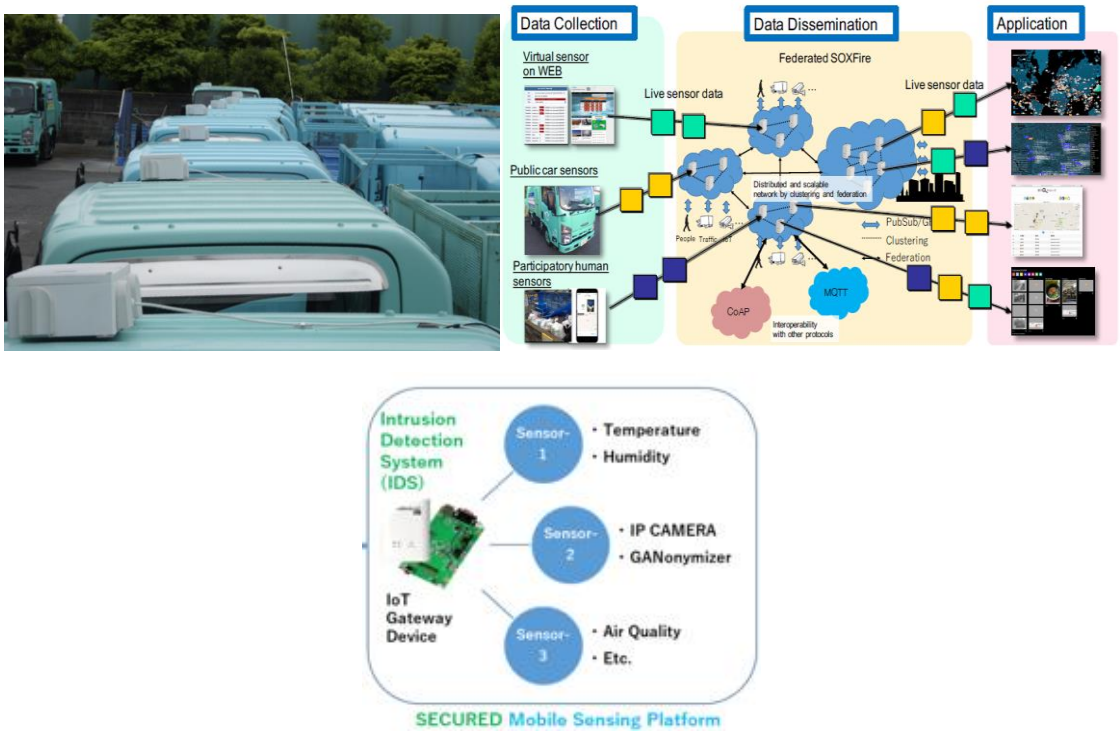

Figure 2—3: Use case 3 Pilot 3 Secure and Trustworthy Mobile Sensing Platform

In this Pilot 3, the environment sensor (temperature and humidity, PM2.5, acceleration sensor, etc.) in the KEIO Mobile Sensing sensor box installed in garbage trucks operated all over Fujisawa city every day, and the image of the in-vehicle camera as input data Flexible analytics app via SOXFire, an advanced sensor platform based on Publish / Subscribe enriched with M-Sec secure and reliable assets, analytics system with deep

learning processing that can operate in edge computing processing environment. For example, we will install secure video processing solution named "Deep Counter". This enables automatic counting the garbage amount by using deep learning engine on the edge computing processing only. It's not necessary to upload the data to the cloud.

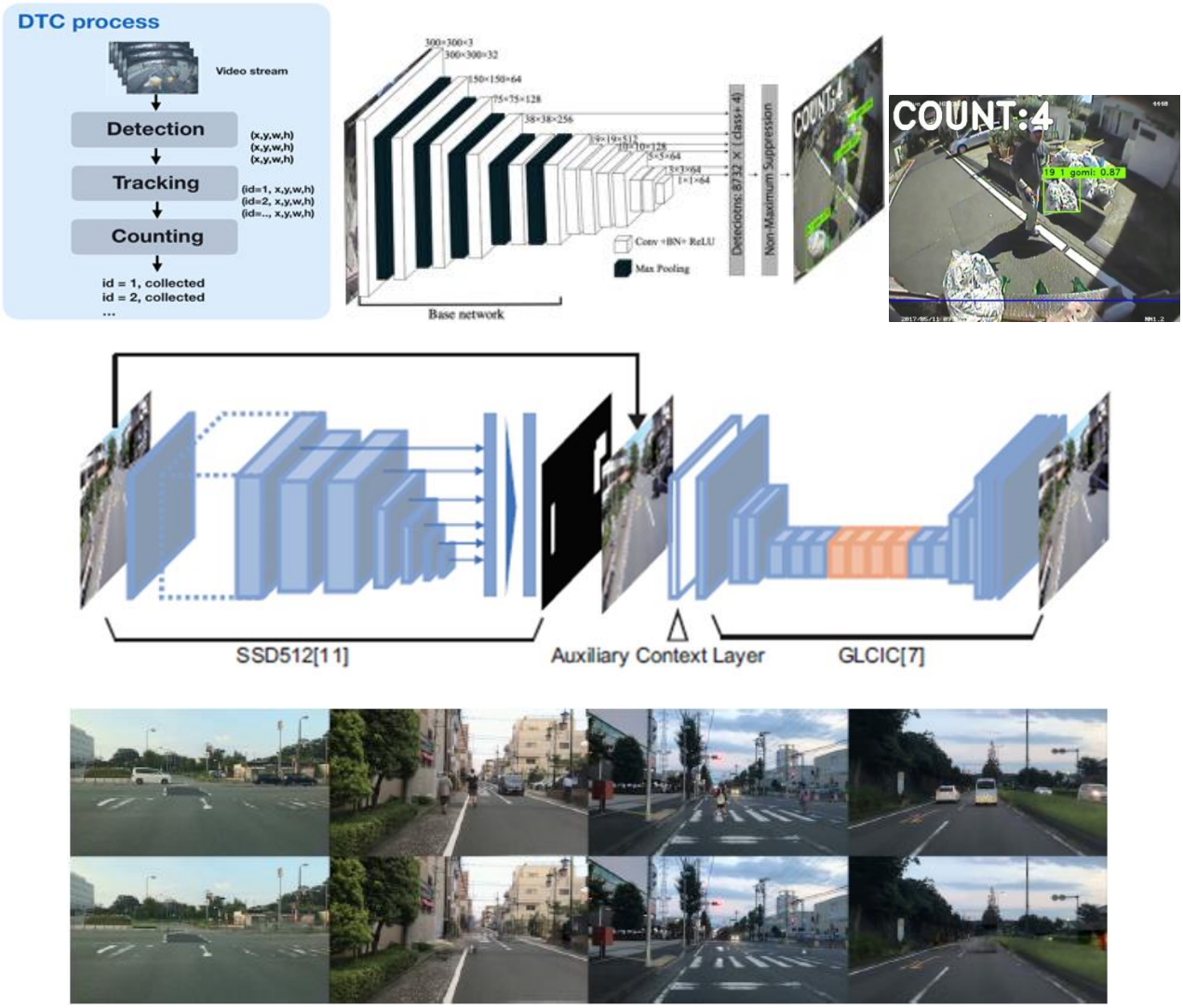

Figure 2—4: Use case 3 Pilot 3 The solution examples of Secure and Privacy protection

The consortium will verify a secure and reliable smart city platform that analyses various cities information using an environment that totally supports the visualization environment including smartphones. UC3 pilot will be focusing on security solution for Keio Mobile Sensing Platform, which is based on off-the-shelf product's common approach of having various sensors coupled with IoT gateway. Since EU side is focusing on the hardware-based security solution in UC-1 and Japan side is focusing on the software-based security solution for off-the-shelf IoT product in UC3, therefore the hardware, firmware, and OS security will be out of scope for UC-3 pilot. Similarly, application will be only for checking Mobile Sensing Platform functionality, and therefore, application security also will be out of scope for UC-3 pilot.

Table 2-22 briefly describes the main aspects of the pilot execution.

Table 2-22: Use case 3 Pilot 3 details

Pilot name	Secure and Trustworthy Mobile Sensing Platform
Location of the pilot	Fujisawa City (Japan)
Users	A total of 22 users will take part of this pilot including 10 garbage collection workers, 2 Fujisawa Municipal officers as well as, 10 citizens..
Infrastructure	• Mobile sensing platform • Secure data delivery platform • Deep Learning processing on edge computing environment • Anonymized Video processing by Deep Learning • Environment monitoring solution
Mobile sensors	• **Weather sensors:** temperature, humidity, pressure, UV-A • **Movement sensors:** acceleration, geomagnetism, angular velocity • **Air sensors:** PM2.5 • **Location sensor**: GPS • **In-Vehicle camera**

2.3.2 Stakeholders' identification

The consortium identified the stakeholders involved within this use case as well as their interest and particular benefits provided by M-Sec in order to establish the communication activities accordingly.

Table 2-23: Use case 3 Pilot 3 stakeholders and participants

Stakeholder	Role	Interested in?	Specific benefits from M-Sec
Garbage collection workers	In charge of garbage collection	Although the automatic counting of garbage by an on-vehicle camera contributes to efficient garbage collection work, as a garbage collection worker, he does not want to see his face in the video data.	By using GANonymizer, it is possible to automatically delete the faces of individuals in order to protect personal data.
Municipal Officers	Responsible for environment monitoring	They would like to improve citizen services by responding quickly to environmental problems. They would like to analyse how, when, and how much waste is discharged to collect garbage efficiently.	UC3 provides precise and detail environmental data that cannot be understood from open data on the Web. Garbage emissions are automatically detected using deep learning with edge computing.

2.3.3 Recruitment criteria

The minimum number of participants per Pilot 3 is 5. They will be recruited from local city government around Shonan Fujisawa Campus of KEIO. Currently the following cities are considered, and under negotiation: Chigasaki City, Samukawa Town, Sagamihara City, Kamakura City, and Yokosuka City.

- **Age of the participants:** ideally between 20 and 65 years old.
- **Gender balance:** ideally 50% female and 50% male participants.
- **Technological capacities:** a balanced mixture of participants including those with good ICT knowledge and those with poor ICT skills is desirable.

2.3.4 Stakeholders' engagement plan

The consortium has created a plan for communication activities among stakeholders in order to achieve engagement and participation to validate M-Sec through Pilot 3. The plan followed is the one provided below:

Table 2-24: Use case 3 Pilot 3 stakeholders recruitment actions

Recruitment Actions	Channel	Target User	Estimated Number of participants	When?	How?	How to keep user engage?
Promotions in KEIO IoT consortium	Physical through the consortium event	General public	20	July 2020	Make a presentation at the event.	Keep providing valuable information to the participants.
Promotions on M-Sec website and social media	Websites, Social Media accounts	General public	100	September 2020	Publish messages through M-Sec website, event website and Fujisawa website when the trial starts.	Keep providing valuable information to the participants.

The consortium so far has engaged ~10 workers for cooperation with this pilot study. The workers are currently in cooperation with KEIO for mobile environment sensing. It also got cooperation from a municipal officer in Fujisawa city to this pilot study.

2.3.5 Data management plan

Table 2-25 shows a summary of the data management plan.

Table 2-25: Use case 3 Pilot 3 data management

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 for 10 years.

2.3.6 Ethics plan

Participants, i.e. city officers and citizens, are recruited via the KEIO IoT consortium events or 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 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 10 years after the end of the pilot as academic evidence of the study.

2.3.7 Set up & Timeframe

Currently the final integration with the M-Sec platform is ongoing. This corresponds to Step 5 in the following table, after which the consortium is planning to start the 1st Trial. Due to the COVID-19 issue, the pilot's starting date of the 1st Trial has been postponed by a few months.

Table 2-26: Use case 3 Pilot 3 Steps assessment process and timeframe

Steps	What	Status	When
Step 1 device development	-Deployment of sensor devices on garbage collection trucks	KEIO Mobile Sensing Platform sensor boxes are installed to Fujisawa garbage collection trucks	M22→ COMPLETED
Step 2 mobile sensing launch	-Connecting the sensor devices with SOXFire sensor data streaming platform	Sensor boxes are connected to SOXFire sensor data streaming platform via 3G network and the Internet.	M26→ ONGOING

Steps	What	Status	When
Step 3 securing mobile sensing system	-Integration with M-Sec platform for security layers	IoT Security M-Sec component has been integrated to the sensor box.	M18-M21→ COMPLETED
Step 4 testing secured mobile sensing system	-Evaluating the behavior of the secured mobile sensing system	The sensor boxes with M-Sec extension showed promising initial integration testing results.	M21-M23→ COMPLETED
Step 5 MVP Release	-Integration of M-Sec platform and secured mobile sensing platform.	Currently the final integration with M-Sec platform is ongoing.	M26→ ONGOING
Step 6 1st Trial	- 1st Trial is initiated.	Due to the COVID-19 issue, the duration of the 1st Trial may be fluctuated.	M27-M28→ NOT INITIATED YET
Step 7 Initial measurement	-KPIs	In order to get an initial benchmark, KPIs will be continuously monitored. Results will be used to enhance the M-Sec components.	M28 → NOT INITIATED YET
Step 8 Sub-iterative releases	-Enhancements and finalization of integration with M-Sec	The integration with M-Sec components will be completely finalized.	M28-M33
Step 9 2nd Trial starts	-Initiation of the second phase of the pilot	Pilot is expected to start in M33 for a total length of 2 months	M33-M34→ NOT INITIATED YET
Step 10 Final assessment	-KPIs	KPIs will be continuously monitored	M35→ NOT INITIATED YET

2.3.8 KPIs

To check the success of Pilot 3, a series of KPIs, listed in the table below, will be monitored.

Table 2–27. Use Case 3 Pilot 3 KPIs

#KPI	Goal	How to measure?	Target	M-Sec Asset
# platform users	Having multiple common platform users as a secure and trustworthiness mobile sensing platform.	Number of platform users	3	SmaileCityReport
# Anonymization	Functional verification of privacy data protection	Number of privacy data erased from video data as privacy data protection	More than 20 privacy-related objects	GANonymizer

#KPI	Goal	How to measure?	Target	M-Sec Asset
# Secure Data Processing	Securely distributes data as a Secure Trustworthiness mobile sensing platform.	Number of data safely delivered as Secure Trustworthiness mobile sensing platform	More than 50 data	Deep Counter Honeypot

2.3.9 Questionnaires

Questionnaires have been considered for participating local government officers. The details will be decided later

2.3.10 Focus Groups

Focus group study is under consideration.

2.3.11 Possible Risks and corrective actions

- Garbage collection service is suspended for a while:
  - Risk: Due to COVID-19, garbage collection service may be suspended if the social status becomes chaotic.
  - Action: In this case we conduct the pilot virtually in KEIO university lab. Benchmarking experiments are still possible with this configuration. Questionnaires and focus groups will be conducted remotely after KEIO explains the UC with remote demonstrations.

2.3.12 User Related Threats

Table below summarizes the non –technical threats associated to pilot3:

Table 2–28. Use Case 3 Pilot 3 User-related threats

Type of User	Potential Threat (non-technical)	Related to a Security Threat	Measures to overcome the threat with M-Sec
Data consumers	Becoming unable to fully optimize their behaviour or make optimum city management decision based on authentic environmental information	- sensors, IoT devices, and cloud systems involved in those data streams are attacked -data are tampered at the attacked subsystem - DDoS attacks make the environmental information unavailable	• T4.1 IoT Security, T4.2 Cloud and Data level Security, and T4.5 Overall end-to-end Security M-Sec components

2.3.13 5Vs definition of Big Data

The following table summarizes the baseline applied to Pilot 3 following the 5Vs definition of Big Data

Table 2-29: Use Case3 Pilot 3 5Vs of Big Data

5Vs	Do the 5Vs appear in the Use Case?/ demo? How?	Would the 5Vs appear in a scaled-up version of the UC? (exaggerated version)	How M-Sec will address/ addresses the 5Vs in the current pilot scenario and the exaggerated scenario.
Volume	Huge amount of sensor data (1GB/day) is transmitted over the end-to-end mobile sensing platform.	Assuming that all garbage trucks over the world are connected to the M-Sec platform, the maximum data volume per day is calculated as follows: 200KB/sec * 60min * 12hours * 350,000trucks = 50TB/day Here we assume 200 garbage trucks exist per 400,000 citizens, which is roughly the case in Fujisawa. Assuming that there are 700 million citizens exist in EU+Japan, the estimated total number of garbage collection trucks is 350,000.	The M-Sec mobile sensing platform generates sensor data 100 times a second.
Velocity	Sensor data must be delivered to the subscribers real-time, e.g., within some miliseconds.	Depending on the sensors used and sensing frequency, the speed becomes over 200KB/sec. If the frequency reaches 2KHz, the required speed is 2MB/sec. This depends, however, on the underlying communication platform in the area.	The M-Sec mobile sensing platform delivers sensor data lively through KEIO SOXFire to their subscribers.
Variety	Different kinds of environmental information are delivered to users.	Different kinds of environmental sensors can be deployed, e.g., those for NOx, SOx, chemicals, etc. There are thousands of different types of sensors corresponding to different chemical materials. The actual data to sense depend on the area to be deployed.	The M-Sec mobile sensing platform contains 10 difference sensors including, for example, accelerometer, compass, PM2.5, temperature, humidity, illuminance, UV. Etc.
Veracity	The sensor data must be trustworthy enough so that the subscribers can decide their activity based on the true environment data.	Sharing trustworthy environmental monitoring data between countries can stack scientifically important data for future research.	The sensor data are protected by M-Sec IoT security mechanism and M-Sec end-to-end security mechanism.
Value	The realtime fine-grained environment information is valuable for residents and travelers.	When this use case covers all over the world, it becomes possible to observe global environment change in a very fine-grained way. Scientific value of such data is priceless.	The sensor data are openly accessible via KEIO SOXFire included in the M-Sec architecture. In addition, data will be transferred to the M-Sec Marketplace.

2.3.14 What M-Sec is offering in terms of security and Why Use Case 3 needs M-Sec?

One of the challenges in this pilot is to clarify whether or not the devices are compromised. Such information enables consumers to know whether the data they see are safe in terms of data authenticity. The nodes in the mobile sensing platform may be hacked, resulting in data integrity issue or becoming a part of DDoS attacks unintentionally. To protect mobile sensing platform from malicious attacks so that the sensing nodes are not hacked and data integrity or availability is not affected. To cope with this problem Intrusion Detection System detects the attacks, and Monitoring&Visualisation Tool make it visible.

Another challenge is to protect the data itself. If the data are, for example, encrypted at the edge side, then it is protected from malicious attackers even if the cloud system is compromised. To address this issue, Secure SOXFire provides end-to-end security, so that the data are transmitted from the source to their destination without being disclosed.

It is also a challenge that we better protect privacy information. If a camera image contains private cars with their numbers and/or individuals with their clear faces, their privacy may be leaked. In these three layers, namely device, data, and data content, secure and trustworthy environment monitoring should be made. This issue is address by Ganonymizer. It automatically deletes objects in an image that are related to such privacy related information.

2.3.15 Four Core M-Sec expected results

Table 2–30 shows how this pilot contributes to deliver the 4 key expected results, highlighting the one to which it contributes the most, Result1.

Table 2–30 Pilot 3 – 4 Core M-Sec expected results

Use case/ Pilot	Title	Result1	Result2	Result3	Result4
Pilot3	Secure and Trustworthy Mobile Sensing Platform	**Yes**	No	Yes	Yes

This pilot contributes mainly to Result1, *'M-Sec distributed, robust and trusted platform'*. Secure mobile sensing platform built atop M-Sec platform provides citizens with trustworthy, distributed, and robust infrastructure for sharing their experiences over the network using the mean of participatory sensing.

Although, it does not directly contribute to Result2, *M-Sec IoT Marketplace* , data coming from this pilot is going to be integrated into the M-Sec marketplace.

Additionally, it contributes to Result3, *'M-Sec smart city ecosystem'.* Secure mobile sensing platform, developed and used in this use case, is an infrastructure upon which new entrants (e.g. startups, SMEs) and other players (e.g. developer communities, students, entrepreneurs) can experiment with the fine-grained data collected from the real world.

Finally, it contributes to Result4, *Revenue model and replication plan*, because UC3's Secure Trustworthiness Mobile Sensing Platform has data distribution capabilities based on SOXFire publish/subscribe model. These capabilities could be base architecture of data exchange business model as a revenue model

2.4 Pilot 4 (Use case 4): Secure Affective Participatory Sensing of City Events

2.4.1 Synopsis of the pilot

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 "SmileCityReport" 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 **¡Error! No se encuentra el origen de la referencia.**. 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, a touristic city spot, etc., depending on the theme specified) 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.

In this Pilot 4, we will have a pilot study firstly in Fujisawa, and next have the second (cross-border) pilot study in Santander as well.

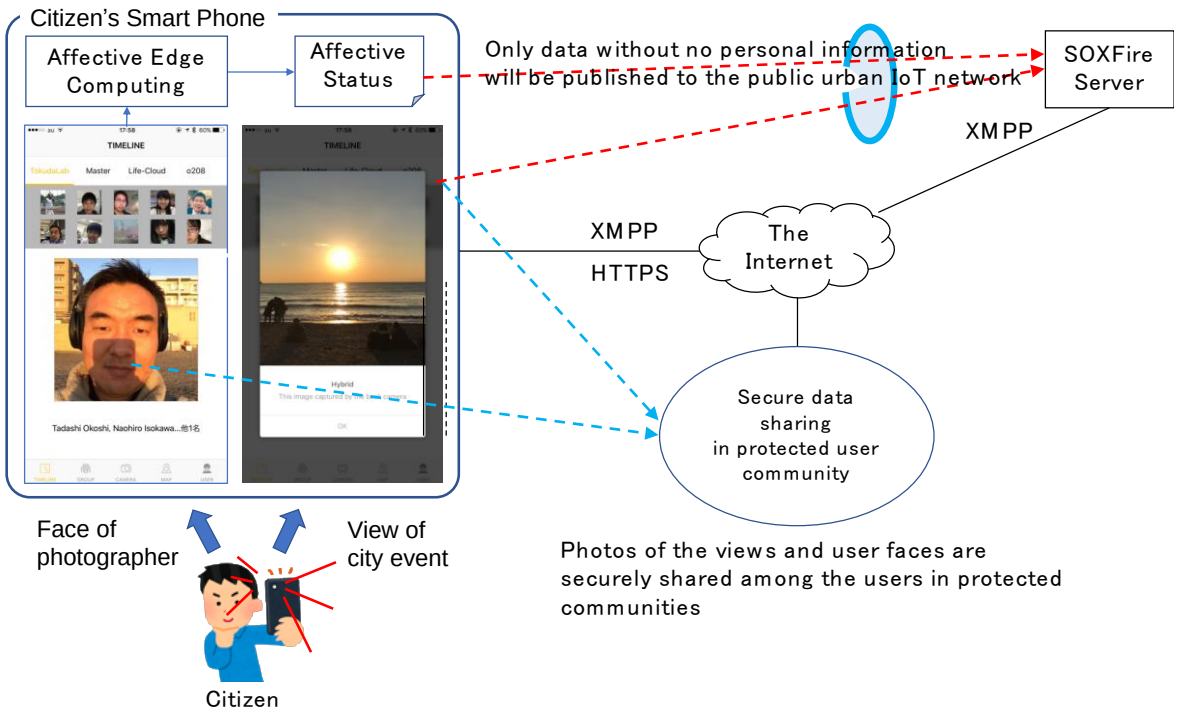

Figure 2—5: Use case 4 Pilot 4

Considering the extension of the pilot to a cross-border one, it has been necessary to take into account the particularities of Santander and Fujisawa in order to define those themes that could be more interesting for citizens of both pilot cities. In this sense, Santander city council is currently working in the development of a new city application, that will include among many other functionalities, the report of events in the city, such as urban furniture in bad condition or full trash cans,.., so this could cause a conflict of interest, as similar functionalities are offered in different apps. Nevertheless, from the perspective of tourism, this pilot could be a driving force for the promotion of tourism by sharing photos between both cities, as well as, for encouraging the international dimension of both pilot cities.

Among the common themes discussed are country specialties, marine plastic waste, virtual sightseeing and virtual gastronomic experiences. Although at the time of edition of this deliverable the common themes are not decided yet, both cities are interested in virtual sightseeing, by exchanging pictures of special spots in Santander and Fujisawa, and gastronomic experiences, by exchanging special drinking and eating spot pictures between both cities. In the case of virtual sightseeing, it may be nice to share beautiful spots of both pilot cities in spring (i.e, cherry blossom in Fujisawa) or summer (i.e., beaches in Santander), allowing participants to show their pride in being a member of their city and to become a kind of ambassador of it. In the case of gastronomic experiences, Japanese partners have identified a gastronomic event, called Chionomi Festival where to promote this pilot. Due to COVID-19, this event has been postponed, however their organizers are interested in joining the pilot once the festival can be held. In the case of Santander, several gastronomic events are held throughout the year, especially in spring and summer. However, due to the coronavirus, all events have been cancelled, so it is necessary to wait for the evolution of this unusual situation, for the tourism council to select the gastronomic event in which the pilot will be promoted.

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

Table 2-31: Use case 4 Pilot 4 Details

Pilot name	Secure Affective Participatory Sensing of City Events (crossborder)
Location of the pilot	Fujisawa City (Japan), Santander City (Spain)
Users	• 2 municipal officers • 10 people to test the new app (phase1, 10 friend-users) and then open it to a larger number of users (phase2, 50 people, including Santander municipal staff and citizens) • Acceptance and consent to participate in this pilot under the conditions expressed by the M-Sec consortium.
Infrastructure	• Affective Participatory Sensing Platform • Secure data delivery platform • Anonymized Video processing by Deep Learning
Mobile devices	• SmileCityReport (client application running on user's smartphone) (projected to support both iOS and Android devices.)

Regarding on the original Pilot 4.2 "Secure Affective Participatory Sensing of City Events" in Use Case 4 "Secure and Trustworthy Hyper-connected Citizens Care" and Use Case 6 "Citizens as sensor" (the use cases proposed originally at the beginning of M-SEC project), these two pilots have been merged and now are positioned as new "Pilot 4 (Use case 4) Secure Affective Participatory Sensing of City Events (crossborder)". During our discussion within the project consortium, one of the key technical components of those original use cases, a system for secure participatory sensing was found to be common among the 2 use cases. Thus we decided to integrate these 2 use cases as "new" use case 4 which also covers crossborder trial between EU and Japan.

2.4.2 Stakeholders' identification

The consortium identified the stakeholders involved within this use case as well as their interest and particular benefits provided by M-Sec in order to establish the communication activities accordingly.

Table 2-32: Use case 4 Pilot 4 stakeholders and participants

Stakeholder	Role	Interested in?	Specific benefits from M-Sec
Municipal Services	Service providers	Municipal officers are interested in promoting their cities. Fujisawa local government and KEIO are collaborating closely in Regional IoT consortium. In Santander, Municipal Tourism service collaborates in defining the pilot study as well as its further development.	Promoting both cities through an app that includes security and privacy mechanisms. Establishing a new communication channel with citizens

Stakeholder	Role	Interested in?	Specific benefits from M-Sec
Citizens	End users of the solution	People interested in discovering or enriching their knowledge in aspects of everyday life in the other pilot city.	Participants from both cities may exchange pictures through an enhanced secure system while by following a gamification approach.

2.4.3 Recruitment criteria

In the case of Santander, close collaboration with the Municipal Tourism Service has enabled to identify potential end users, including municipal staff, such as representatives from Tourism municipal service, and IT department, people from the tourism sector, as well as, general public, by contacting neighbourhood associations and volunteer citizens who have participated in other pilot experiences.

- **Working status:** For the first trial of this pilot, a group of 10 friend-users from the groups identified above will be involved.
- **Minimum age of the participants:** 18 years old is the minimum required age to participate in this pilot.
- **Gender balance:** ideally 50% female and 50% male participants.
- **Technological capacities:**
    - The participant needs to know how to handle conventional smartphones.
    - The participant needs to have his/her own smartphone.

2.4.4 Stakeholders' engagement plan

The consortium has created a plan for communication activities among stakeholders in order to achieve engagement and participation to validate M-Sec through Pilot 4. The plan followed is the one provided below:

Table 2-33: Use case 4 Pilot 4 stakeholders recruitment actions

Recruitment Actions	Channel	Target User	Estimated Number of participants	When?	How?	How to keep user engage?
Promotions in KEIO IoT consortium	Physically through the consortium event	General public	20	July 2020	Make a presentation at the event.	Keep providing valuable information to the participants.
Promotions on M-Sec website and social media (Fujisawa & Santander)	Websites, Social Media accounts	General public	100	TBD when the promotional events take place	Publish messages through M-Sec website, event website, Fujisawa	Keep providing valuable information to the participants.

Recruitment Actions	Channel	Target User	Estimated Number of participants	When?	How?	How to keep user engage?
					website and Santander website when the trial starts.	
Focus group	F2F meeting	General public	20	TBD when the promotional events take place	A meeting to present the Use Case to the public.	Keep providing valuable information to the participants.
Collaboration with Municipal Tourism Service	F2F meetings and online channels	Municipal tourism service	3	Second year of the project and on-going	Periodic conversations with Municipal Tourism Service representatives to identify potential end-users as well as to promote their participation	Taking into account their expertise in this area and in previous pilot experiences, they are actively participating in aspects such as the definition of common themes and providing Santander merchandising as reward for participants.
Focus group (Santander)	F2F meeting	General public, municipal staff, tourism sector staff, neighbourhood associations, citizens who have participated in other pilot experiences.	10	Sept-Oct2020	A meeting to present the Use Case to the public.	Keep providing valuable information to the participants.

The consortium so far has engaged 2 municipality workers and 1 NPO organization in the local Fujisawa area for cooperation with this pilot study. We have been discussing possible pilot scenario so far, however, due to the recent COVID-19 pandemic situation, more re-consideration/ re-planning of the cooperation would be needed.

2.4.5 Data management plan

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

Table 2-34: Use case 4 Pilot 4 data management plan

Type of data	• Photo data: (1) photographer's facial photo, (2) city event's photo • Estimated affective data: (1) smile degree of the photographer, (2) smile degree of the photo viewer • Other sensor data: Smartphone sensor data such as (1) activity recognition, (2) light sensors, (3) accelerometer, (4) gyroscope, (5) magnetometer etc. etc. • Location information: (3) location information of the photo venue • User profile: (1) age range, (2) gender, (3) occupation, (4) residential area • Network address: (1) IP addresses of the users • Survey answer: (1) survey answer
Format of data	• Photo data: Image data (JPEG) • Estimated affective data: Integer/Double values • Other sensor data: Double values (individually) • Location information: Double values (longitude / latitude) • User profile: Text and numerical values • Network address: IP address structure • Survey answer: text
Data collection	• Data: sensed by cameras and sensors of user's smartphone • Survey: Through survey web page
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 for 10 years.

2.4.6 Ethics plan

On overall ethics aspect of this pilot will be reviewed and approved by IRB of one of the partners of M-SEC consortium. Ethical approval will be granted by Keio University.

During this registration stage, the user is first informed about the main concepts of the data protection, such as who the controller is, which the purpose of data collection is, what the legitimacy is, who the recipients are, as well as which their rights are; and then, they will authorize the data processing. Only when the user accepts this basic information, can they continue with the registration in the app. Also, the participants can uninstall the application at any time.

Furthermore, data protection issues with handling of personal data will be addressed by the following strategies:

- Volunteers to be enrolled will be given comprehensive information, so that they are able to autonomously decide whether they consent to participate or not.
- The data gathered through the application will be stored in pseudonymized form. Questionnaire survey will be conducted in anonymization basis.
- The access logs will be used for research purposes only.
- All the data collected during this pilot will be stored in KEIO for 10 years after the end of the pilot as academic evidence of the study.

2.4.7 Set up & Timeframe

Currently the final integration with the M-Sec platform is ongoing. This corresponds to Step 2 in the following table, after which the consortium is planning to start the 1st Trial. Due to the COVID-19 issue, the starting date for the 1st Trial may be postponed by a few months.

Table 2-35: Use case 4 Pilot 4 Steps assessment process and timeframe

Steps	What	Status	When
Step 1 SmileCityReport development	Development of SmileCityReport	The development is approaching to the end and expected to be done by M26.	M18-M26→ ONGOING
Step 2 Integration	-Integration among SmileCityReport, Ganonymizer and SOX.	Integration between SmileCityReport and Ganonymizer, SmileCityReport and SOX will be done by M26.	M24-M26→ ONGOING
Step 3 Pilot preparation (Fujisawa)	- The concrete planning of pilots in Fujisawa - Approval from NICT on personal data handling - IRB Approval from Keio University	The initial discussion with NPO and Fujisawa city started M16-M17. Due to COVID-19, re-designing the pilot is required and under going.	M16-M28→ ONGOING
Step 3 Pilot preparation (Santander)	The concrete planning of pilots in Santander	The initial discussion with NPO and Santander city started M16-M17. Due to COVID-19, re-designing the pilot is required and under going.	M16-M30→ ONGOING
Step 5 MVP Release	The integrated components for the 1st Trial	Will be released and going on the deployment for the pilot.	M27→ ONGOING
Step 6 1st Trial starts	1st Evaluation	Pilot is expected to start in M28 for a total length 1 month.	M28 (projected but not fixed, due to progressing

Steps	What	Status	When
			situation in CODIV-19)
Step 7 Initial measurement	-KPIs -Questionnaires	Questionnaires and KPIs will be analysed. The results will be used to enhance the M-Sec components.	M29→M30 (projected but not fixed, due to progressing situation in CODIV-19)
Step 8 Sub-iterative releases	-Enhancements and finalization of integration with M-Sec	The integration with M-Sec components will be completely finalized.	M29→M32 (projected but not fixed, due to progressing situation in CODIV-19)
Step 9 2nd Trial starts	2nd Evaluation	Pilot is expected to start in M33 for a total length 1 month.	M33 (projected but not fixed, due to progressing situation in CODIV-19)
Step 10 Final assessment	-KPIs -Questionnaires	Assessing Questionnaires and KPI during the 2nd study	M34→M36 (projected but not fixed, due to progressing situation in CODIV-19)

2.4.8 KPIs

The table below lists a series of KPIs that will be monitored in order to check the success of Pilot 4.

Table 2–36. Use Case 4 Pilot 4 KPIs

#KPI	Goal	How to measure?	Target	M-Sec Asset
# of privacy-related objects filtered out from input images	To evaluate the volume of data from which privacy-related objects have been filtered out	Counting the number of processed images in the component.	More than 70% of the objects that the filtering component originally targeted.	Ganonymizer
# of objects going to SecureSOXFire	To evaluate how much data objects to be input into the public smart city network	Number of data (post object)	100	SecureSOXFire

2.4.9 Questionnaires

Questionnaires are under consideration for this pilot. Whether they will be used or not will be decided later.

2.4.10 Focus groups

A focus group will be conducted at the end of the trial with friend users in order to get their. Their opinions and experiences maybe valuable inputs into WP4 for the next iteration of the trial.

2.4.11 Possible risks and corrective actions

- Number of participants:
  - Risk: The pilot does not acquire the desired number of participants.
  - Action: This pilot will be initially validated with small number of end users, considered people close to the partners involved in the experience. Then, the recruitment of citizens will take place through different actions in order to reach a higher number of participants. At this stage, a rewards system will be implemented, to attract a larger audience.

2.4.12 User Related Threats

The table below summarizes the non –technical threats associated to pilot4:

Table 2–37. Use Case 4 Pilot 4 User-related threats

Type of User	Potential Threat (non-technical)	Related to a Security Threat	Measures to overcome the threat with M-Sec
Data producers Data consumers (end users)	Being not attracted to use this application	- Personal data of SmileCityReport user (reporting user) will be leaked to the public (e.g., His/her facial image, taken by a smartphone's inner camera, will be accidentally sent to the public network, due to unclear explanation / user-interface on the application, and/or due to user's mistake in their application operations.	• Creating easy-to-use joy-to-use user interface and facutionalities in SmartCityReport implementation • Well design the field trial with external collaborators/partners and Fujisawa city in the field trial area, to attract the participants to join the study as whole.
Data consumers	Becoming unable to fully optimize their behaviour or make optimum city management decision based on authentic environmental information	- Personal data of SmileCityReport user (reporting user) will be leaked to the public (e.g., His/her facial image, taken by a smartphone's inner camera, will be accidentally sent to the public network). - Personal data of people (accidentally taken inside the photo by a reporting user) will be leaked to the public (e.g., His/her facial image, taken by the reporter user's smartphone's outer camera, will be accidentally sent to the public network) - Personal data of SmileCityReport user (viewing user) will be leaked to the public (e.g., His/her facial image, taken by a smartphone's inner camera, will be accidentally sent to the public network	• T4.2 Cloud and Data level Security, and • T4.5 Overall end-to-end Security M-Sec components

2.4.13 5Vs definition of Big Data

¡Error! No se encuentra el origen de la referencia. summarizes the baseline applied to Pilot 4 following the 5Vs definition of Big Data

Table 2-38: Use Case4 Pilot 4 5Vs of Big Data

5Vs	Do the 5Vs appear in the Use Case? How?	Would the 5Vs appear in a scaled-up version of the UC? (exaggerated version)	How M-Sec will address/ addresses the 5Vs in the current pilot scenario and the exaggerated scenario.
Volume	Yes, assuming that every user posts 5 pairs of photo posts (= 10 photo data) to SmileCityReport, and assuming 10 users use this system, 100 photos will be posted / day.	In Japan 79,370,000 people are estimated to use social networking in 2020. Assuming those people use the system every day with 1 photo post → 79,370,000 photo data/ day	SmileCityReport is using elastic cloud infrastructure to achieve such scalability. SOXFire can be federated to achieve such scalability.
Velocity	Yes, assuming that every user posts 5 pairs of photo posts (= 10 photo data) to SmileCityReport, and assuming 10 users use this system, velocity will be "10 posted / day".	In Japan 79,370,000 people are estimated to use social networking in 2020. Assuming those people use the system every day with 1 photo post → Velocity will be "79,370,000 photo data/ day" (="367 photos / sec")	SmileCityReport is using elastic cloud infrastructure to achieve such velocity. SOXFire can be federated to achieve such velocity.
Variety	N/A	N/A	N/A
Veracity	Trustworthy and appropriateness of reported photo data	In case that this system will deployed in a very large scale, unfortunately potentially there may be certain number of people with intention of positing in-appropriate content are expected to be joining to the system.	Introducing the concept of social network and "like" mutual recognition so that the more trustworthy data will be recognized more. ' Introducing the features of "black listing" "banning" on the system so that in-appropriate content will be properly banned.
Value	The number of business related participants during the field study. Degree of evaluation to the system by such participants	Assuming all the businesses in each city uses this system, all city event data with privacy-erased data will be published to public smart city network. Thus very fine-grained smart city event mapping will be possible.	Jointly promote the advertisement of the field study to such class of potential participants

2.4.14 What M-Sec is offering in terms of security and Why Use Case 4 needs M-Sec?

Challenge in this pilot study is protecting people's privacy-related information, mutually among different members of affective participatory sensing system, yet providing adequate quality of information (not including the privacy but including certain "affective" status information) to the public smart city network which are preferable to be utilize in the local smart city/area's reviewing. Examples of such privacy-relate information is the face of people (those who reports the city event, and those whose face is coincidently taken by a city-report photo), and facial expression such as smile expression.

For the former, the M-SEC platform especially Ganonymizer component erases such faces from the photo data and protect such people's privacy. For the latter, SmileCityReport and SecureSOXFire only shares the numeric number of affective status (e.g., degree of smile) extracted from the original facial expression photo data, to the public smart city sensor network to protect the people's privacy. In those ways, M-SEC provides a novel privacy-protection security features and mechanisms to the affective participatory sensing scenario which has a big potential as the latest smart city applications.

To achieve overall security for such application scenario, various types of technical components will be needed. Also, possible difference of sense of privacy between different countries may have additional value as a research. For such reasons, this use case definitely needs M-SEC project.

2.4.15 Four Core M-Sec expected results

¡Error! No se encuentra el origen de la referencia. shows how this pilot contributes to deliver the 4 key expected results, highlighting the one to which it contributes the most, Result1.

Table 2–39 Pilot 4 – 4 Core M-Sec expected results

Use case/ Pilot	Title	Result1	Result2	Result3	Result4
Pilot4	Secure Affective Participatory Sensing of City Events (crossborder)	**Yes**	No	Yes	Yes

This pilot contributes mainly to Result1, *'M-Sec distributed, robust and trusted platform'*. Smart City Report application built in top of M-Sec platform provides citizens with trustworthy, distributed, and robust infrastructure for sharing their experiences over the network using the mean of participatory sensing.

Although, it does not directly contribute to Result2, *M-Sec IoT Marketplace* , data coming from this pilot is going to be integrated into the M-Sec marketplace.

Additionally, it contributes to Result3, *'M-Sec smart city ecosystem'.* Smart City Report, developed and used in this use case, is an infrastructure upon which new entrants (e.g. startups, SMEs) and other players (e.g. developer communities, students, entrepreneurs) can experiment with the data collected from citizens.

Finally, it contributes to Result4, *'Revenue model and replication plan',* in that the application built in this use case can be a seed to start a new way of exchanging data between citizens and stakeholders. Looking at the

application as a distributed participatory sensing service, the ecosystem should be the data/money loop between the participating citizens and stakeholders who buy the data from the M-Sec marketplace.

2.5 Pilot 5 (Use case 5): Smart City Data Marketplace with secure Multi-layer Technologies

2.5.1 Synopsis of the pilot

Pilot 5 will be carried out in both cities Santander and Fujisawa, in order to construct a marketplace between EU and Japan to distribute data by ensuring Confidentiality, Integrity, Availability, and Privacy of data following GDPR/APPI regulations, so that people or organisations in EU and Japan can utilize the data more effectively.

Recently, the demand for foreign business is increasing all over the world. Business opportunities are expected in a variety of situations. In such circumstances, data distribution between countries needs to take place safely and smoothly done to make the data effective enough to contribute to “building” the smart city.

Along with the development of the Internet, cyber-attacks are becoming increasingly complicated and sophisticated, provision of a secure data distribution method between countries is an essential task for smart cities.

The aim of this use case is to construct a marketplace where data integrity is present and tamperproof data can be securely distributed with secure multi-layer technologies.

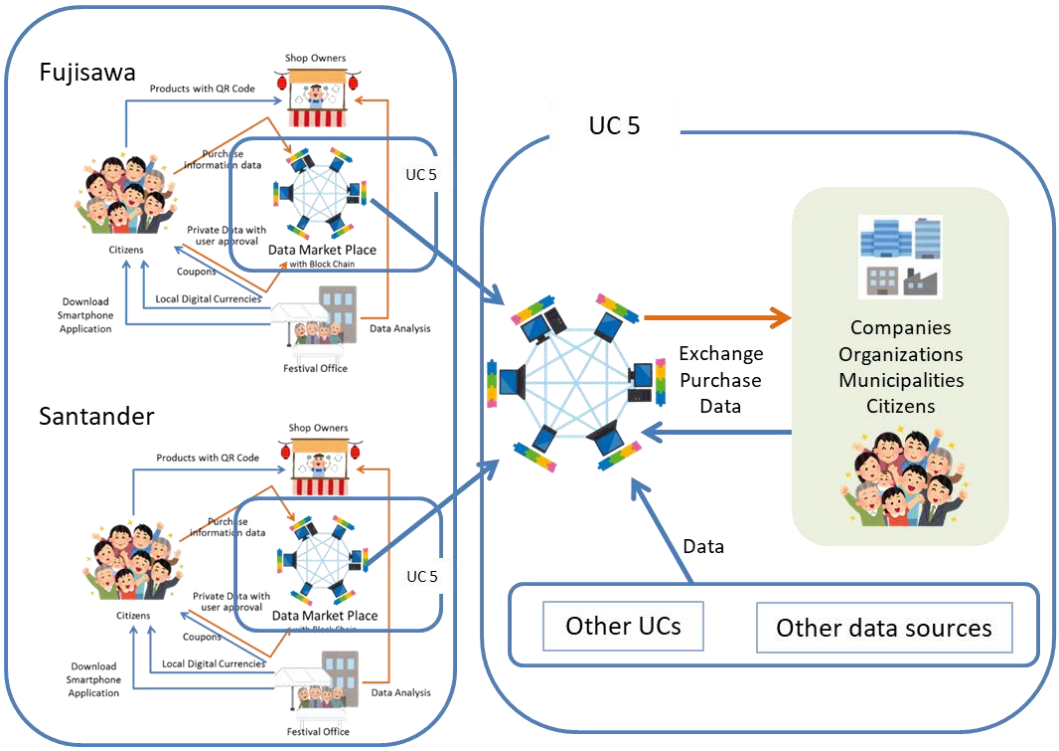

Figure 2—6: M-Sec marketplace image

Table 2-40 describes briefly the main aspects of the pilot execution.

Table 2-40: Use case 5 Pilot 5 Details

Pilot name	Smart City Data Marketplace with Secure Multi-Layer Technologies
Location of the pilot	Fujisawa City (Japan) , City of Santander (Spain),
Infrastructure	IoT Marketplace application
IoT Sensors	Sensorizer and sensors related to use case 1 – 4.

2.5.2 Stakeholders' identification

The consortium has identified the stakeholders involved within this use case as well as their interest and particular benefits provided by M-Sec in order to establish the communication activities accordingly.

Table 2-41: Use case 5 Pilot 5 Stakeholder Identification

Stakeholder	Role	Interested in?	Specific benefits from M-Sec
Citizens	Data providers and buyers	Environmental data of the cities to know about the city and what's going on. Home activity data, to compare the activities of the ageing people. Also providing and buying photos of the cities and events.	M-Sec will provide the security and reliability on protecting the data provided from the citizens in a secure way.
Universities and Research institutions	Data providers and buyers	Information to research the characteristics of the area is available, and can sell their research results.	Universities and Research institutions can be provided with data where data integrity is present and tamperproof data can be securely distributed with secure multi-layer technologies.
Cities	Data providers and buyers	When the municipality or an organization is responsible for the management of a festival/event, they can keep track of what's going on during a festival/event, and also during normal times for planning purposes. The municipality can sell and buy valuable information with people who want to know the city more.	Reliable and secure data is available and can provide data in a safe and secure environment.
Companies	Data providers and buyers	Information is available to companies, event planners, and others who are considering business to research the characteristics of the area. Companies can sell their own unique information and also buy information or aggregated data to utilize on their buiness such as analysing them to make dicisions for	

Stakeholder	Role	Interested in?	Specific benefits from M-Sec
		commercializing products.	

2.5.3 Recruitment criteria

Marketplace participants are data buyers and data providers who need/can provide specific data. Expected participants are citizens, municipalities, companies, research institutions, etc. As it is an online exchange, they need a certain level of IT literacy and devices such as computers or smartphones with network environment to exchange data. A stable network environment is preferable because data exchange of photos and movies is also expected.

- **Working status:** For the first trial of this pilot, the consortium will be focused on local stakeholders from both cities.
- **Minimum age of the participants:** Although in the case of Japan, there is no minimum age requirement for participants, in the case of Europe, 18 years old is the minimum required age to participate in this pilot.
- **Gender balance:** although there is no specific requirement regarding gender, ideally 50% female and 50% male participants.
- **Technological capacities:** Since the smart contract interface to be used in the marketplace has been designed to be user friendly, the only requirement could be to know how to handle a mobile device.

2.5.4 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 and test it further with event organisers and companies that are interested into it.

Table 2-42: Use case 5 Pilot 5 stakeholder recruitment actions

Recruitment Actions	Channel	Target User	Estimated Number of participants	When?	How?	How to keep user engage?
Promotions on M-Sec website and social media	Websites, Social Media accounts	General public	100	TBD when the UC1-4 trial begins	Publish messages through M-Sec website, event website and city websites when the trial starts.	Keep providing valuable information to the participants.
Flyers of events (Collaboration with the event in use	Physically (through the event organizer)	General public	100	TBD when the UC1-4 trial	Distribution by the event organizer during the event.	Providing interesting themes that make for fascinating photos that people will want to buy.

Recruitment Actions	Channel	Target User	Estimated Number of participants	When?	How?	How to keep user engage?
case 4)				begins		
Focus group	F2F meeting	General public	20	TBD	A meeting to present the Use Case to the public.	
Presentation of the Use Case (focusing on the application and the security on it)	Webinar	General public	20	TBD	A meeting to present the Use Case to the public.	Keep providing valuable information to the participants.
Collaboration with Municipal Innovation Manager and head of IT service	F2F meetings and online channels	Municipal Innovation & IT areas	5	End of the second year of the project and ongoing	Periodic conversations with Innovation & IT representatives to identify potential end-users as well as to promote their participation	Taking into account their expertise in previous pilot experiences, they participate in identifying potential users, such as SME´s, local developers and research institutions.

2.5.5 Data management plan

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

Table 2-43: Use case 5 Pilot 5 Data Management

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 Companion Database
Data management	• All the data stored during the pilot will be kept during the project life time.
Data management	• The anonymity and privacy of participants must be respected. Personal

principle	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. • In case the data provider requests deletion of the data provided, the data must be deleted or the access to them must be impossible for others, without any undue delay. • 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.

2.5.6 Ethics plan

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

- No privacy-related information is collected, nor personal data processed.
- 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 in the other use cases will be stored, without any personal data, in the encrypted database and after the end of the project, the data will be deleted.

2.5.7 Set up and timeframe

- Data collected in M-Sec use cases, sensor data, environmental data, etc. are aggregated in the companion database and those data will be exchanged in M-Sec marketplace.
- For marketplace validation, Smile City Report and Marketplace are directly integrated and the data collected from Smile City Report is exchanged in the marketplace as the first step. Data collection will be verified as UC4, and data exchanging in the marketplace will be verified as UC5.
- Marketplace users will be recruited from webinars, workshops, conferences and more. Furthermore, with the cooperation of both Santander and Fujisawa cities, we are also looking for participants at conferences and events in the cities.
- For data exchanging in the marketplace, tokens or coupons specially prepared by M-Sec will be used as the value, but details are under consideration.

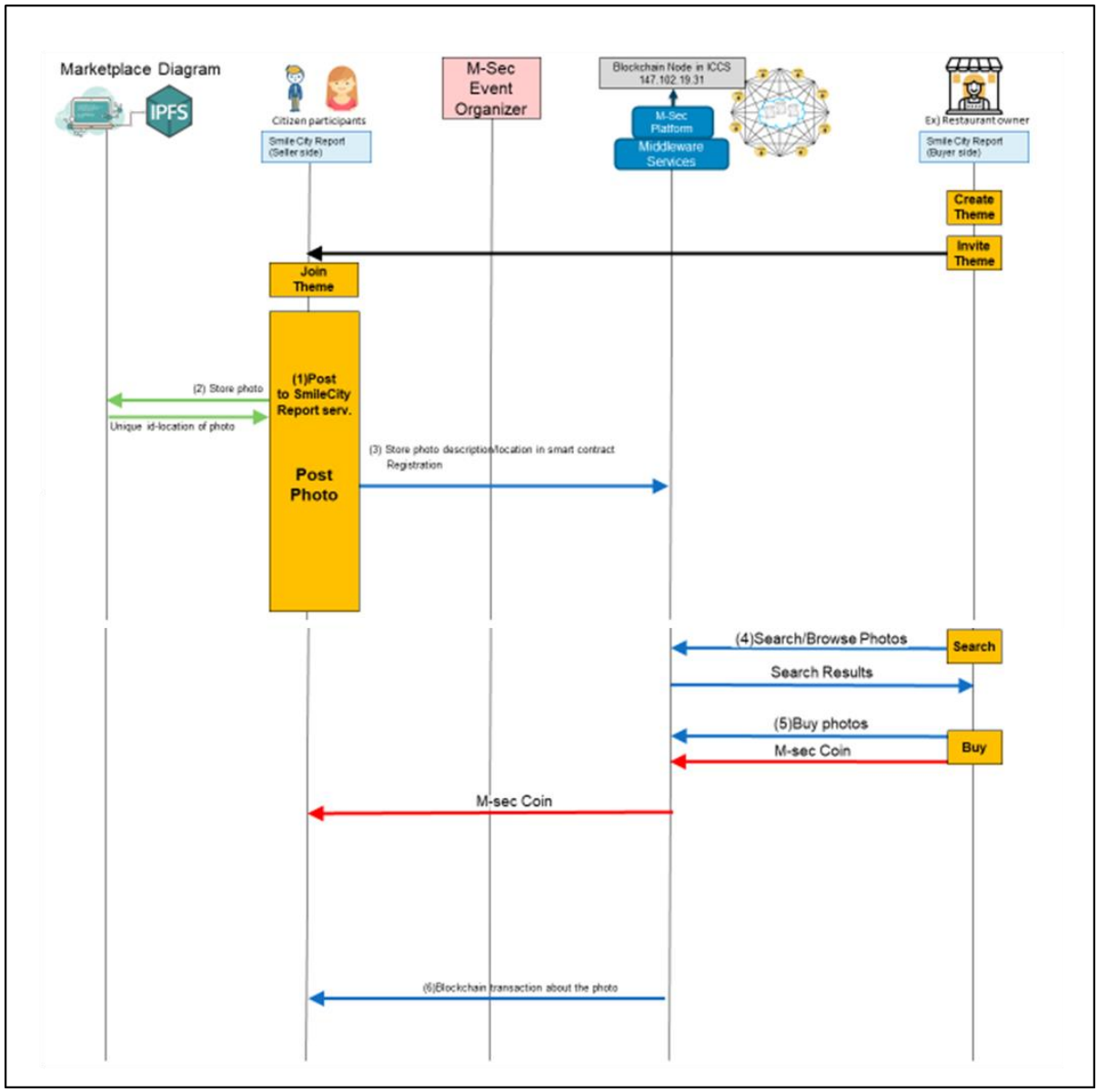

Figure 2—7: Use case 5 Pilot 5 Marketplace Diagram

Table 2-44: Use case 5 Pilot 5 Steps assessment process and timeframe

Steps	What	Status	When
Step 1 Preparation	Development of Maketplace Integration and aggregation of other UC data	Discussions the scenario between both technical and use partners part.	M23-M30→ONGOING
Step 2 Recruitment	Promotion of the Field Trial (FT)	Discussing Promotion ideas with stakeholders	M23-M34 (projected but not fixed, due to progressing situation in CODIV-19)
Step 3 Integration	Smile City Report + Marketplace integration.	Planning and preparing how to integrate between ICCS and Keio	M27
Step 3 1st Trial	1st Field Trial Implementation -	Same as above	M28-M30 (projected but not fixed, due to progressing situation in CODIV-19)
Step 4 Evaluation	1st Evaluation	Not started yet	M31-M32 (projected but not fixed, due to progressing situation in CODIV-19)
Step 5 Preparation	Preparation for 2nd trial	Not started yet	M31-M33 (projected but not fixed, due to progressing situation in CODIV-19)
Step 6 2nd Trial	2nd Field Trial Implementation – Analysis of the results.	Not started yet	M34-M36 (projected but not fixed, due to progressing situation in CODIV-19)
Step 7 Final assessment	-KPIs -Questionnaires	Assessing Questionnaires and KPI during the 2nd study	M36-M37 (projected but not fixed, due to progressing situation in CODIV-19)

2.5.8 KPIs

To check the success of Pilot 5 a series of KPIs, listed in Table 2-45, will be monitored.

Table 2-45: Use case 5 Pilot 5 KPIs

#KPI	Goal	How to measure?	M-Sec Asset
#of transactions	>10000	Get stakeholders involved and motivate them to sell and buy data (or just exchange them)	Marketplace
# of data resources	>1000	Upload data from all the use cases' FT, utilize sensorizer.	Marketplace Companion Database

# of users	>100	According to the recruitment criteria, we will have webinars, workshops and so on to gather the participants.	Marketplace
# of engaged businesses / organizations (e.g. accepting the coupons system)	>10	Get stakeholders involved and motivated.	Marketplace
% non-malicious entities at the Marketplace	>51	By using permission mechanisms and trust & reputation model.	Marketplace & M-Sec blockchain
Limit of requests from DDoS attacks	<10.000 (number of transactions per second that the blockchain can handle)	Using "gas" for these transactions, thus making an attack that could have exceeded the capabilities of the platform too expensive.	Marketplace & blockchain
% Net promoter scoring	>70	Through a questionnaire, more focused on net promoter score.	Marketplace

2.5.9 Questionnaires

Questionnaires have been considered for Marketplace participants. The details will be decided later.

2.5.10 Focus Group

A focus group will be conducted at the end of the trial. It will involve 5 to 10 people plus a moderator who will lead the exchange of ideas based on 10-15 questions where the main purpose will be that each participant expresses their ideas and opinions.

2.5.11 Possible risks and corrective actions

- Participants' interests:
  - Risk: People may not be interested in using the applications (no interest in providing /sharing /buying /selling data in the marketplace).
  - Action: Add valuable information to motivate stakeholders. Include points/coupons/ranking system. Coupons could be redeemed in specific businesses. Advertise the fun aspects of the applications.

- Protection of personal data:
  - Risk 1: People may be interested in using the application but may be afraid of sharing their

data because they are worried about leaking the data:

- Risk 2:Data reliability may not be guaranteed
- Action: The purpose of M-Sec is to avoid any malicious attack or breach of personal data. Therefore, M-Sec components integrated within the solution of all the use cases will provide extended security measures to avoid any risk related to it. Additionally, minimization principles have been applied in order to minimize the use of personal data only to what is strictly necessary for the technical evaluation. And the security aspects of the applications should be "advertised" and made known to the users, in a user-friendly manner.

2.5.12 User Related Threats

The table below summarizes the non –technical threats associated with pilot5:

Table 2–46. Use Case 5 Pilot 5 User-related threats

Type of User	Potential Threat (non-technical)	Related to a Security Threat	Measures to overcome the threat with M-Sec
Data providers and Data buyers	Selling and buying inappropriate data	- Personal data of the other use cases accidentally sent to the encrypted data base (e.g., identifiable photos or photos of a facial image). - Sensors, IoT devices, and cloud systems involved in each use cases are under attack .	• All security tasks (T4.1-T4.5)
Data providers and Data buyers	Selling and buying inaccurate data	- Sensors, IoT devices, and cloud systems involved in each use cases are under attack. - Tampered data sent to the encrypted database - Inappropriate quality data provided	• All security tasks (T4.1-T4.5)
Data providers and Data buyers	Marketplace does not provide relevant value added to attract both users	Lack of confidence to the system	• All security tasks (T4.1-T4.5) and business model.

2.5.13 5Vs definition of Big Data

Table 2-47 summarizes the baseline applied to Pilot 5 following the 5Vs definition of Big Data

Table 2-47: Use Case5 Pilot 5 5Vs of Big Data

5Vs	Do the 5Vs appear in the Use Case? (current pilot)	Would the 5Vs appear in a scaled-up version of the UC? (exaggerated version)	How M-Sec will address/ addresses the 5Vs in the current pilot scenario and the exaggerated scenario.
Volume	Yes, the data collected in	The amount of data in	Depending on the use case and pilot or

	other UCs as well as the data collected by the Sensorizer will also be connected to the marketplace.	exaggerated version would be aggregation of data from the other use cases. The goal of Marketplace participants is 100 total in Santander and Fujisawa. This about 0.017% of combined population of both cities. (170K in Santander, 430K in Fujisawa) If it applies to 2 countries, it would be 28,000 participants. (47M in Spain, 1.2B in Japan）	application, different encrypted DBs and blockchains will be used. Depending on the volumes of data, new nodes could be used, thus ensuring the successful handling of large amounts of data.
Velocity	Yes, the transaction should be approved quickly especially when trading real time data.	NA	By using hyperledger, 100K transaction/sec is possible.
Variety	Yes, a wide variety of sensors will participate in the marketplace.	If the marketplace gets the more data providers, the wider variety of data is going to be available. If the data provider participants is 2 times more, we can assume the variety of data will be 2 times.	By using Sensorizer and secure SOXfire.
Veracity	Yes, by ensuring the legitimacy of a transaction.	NA	Use M-Sec blockchain to prevent falsification, and KYC service which will be a part of it, to identify users. A Trust & Reputation model may also be used to increase the reliability of the shared content per sec.
Value	Yes, by considering the security requirements of GDPR and APPI as a cross-border UC. Can also add value by analyzing data or cataloguing with metadata.	NA	This will be handled by the M-Sec business model and analysis task.

2.5.14 What M-Sec is offering in terms of security and Why Use Case 5 needs M-Sec?

This UC will handle all data from other UCs. In case personal data are included, they will be protected from falsification and be transferred in a secure environment. The system needs to be able to avoid and face attacks to the blockchain and the actual marketplace. The marketplace needs to be operated in a secure environment using M-Sec which will consider the security requirements of GDPR and APPI. Indicatively, M-Sec has conducted a lot of research on coupling encrypted databases with blockchain technologies, thus making the synergy of off-chain and on-chain storage and processing of data possible, a characteristic which enhances security considerably, while still ensuring data reliability and users' privacy. Also, the integration of a Trust and Reputation system within the blockchain implementation is considered, which, to our knowledge, is an innovative feature. While all the other mechanisms provided by M-Sec are part of what is known as hard security, a Trust & Reputation model covers the need for soft security* (which refers to social control mechanisms). By evaluating the data-providers and using Trust and Reputation indexes, it becomes possible to identify which actors of the ecosystem may provide data with low credibility. Thus, by using feedback/evaluations of the services from the data-consumers, it becomes possible to protect them from future "consumption" of harmful or false data.

2.5.15 Four Core M-Sec expected results

Table 2–48 shows how this pilot contributes to deliver the 4 key expected results, highlighting the one to which it contributes the most, Result2.

Table 2–48 Pilot 5 – 4 Core M-Sec expected results

Use case/ Pilot	Title	Result1	Result2	Result3	Result4
Pilot5	Smart City Data Marketplace with secure Multi-layer Technologies	Yes	**Yes**	Yes	Yes

This pilot contributes mainly to Result2, *M-Sec IoT Marketplace*. The main purpose of this pilot is to build IoT marketplace utilizing multi-layer security technology including blockchain for citizens, companies and municipalities to exchange data in the secure environment.

The data that will be exchanged in this marketplace is all the data collected in the other UCs as well as sensor data collected by sensorizer. This contributes Result 1, *M-Sec distributed, robust and trusted platform* because of the security provided by blockchain and also the security mechanisms included on other use cases to make the data sent to the Marketplace reliable.

It also contributes Result 3, *M-Sec smart city ecosystem*, to attract stakeholders such as IoT providers, developers, and companies, because the data could be utilized in variety ways and in circulation.

And, it contributes to Result4, *Revenue model and replication plan*, since services that allow citizens, companies, local governments, etc. to freely exchange the necessary data in a secure environment are not widely spread at present. This pilot will be one way to help to promote future data utilization society. We will seek to create a business model.

3 Conclusions

This document provides a report of the M-sec pilots, detailing the main activities carried out during the second year of the project in both pilot cities, Santander and Fujisawa.

As due to the coronavirus the M-Sec pilots have not been able to start on the foreseen date, the consortium has decided to divide this report in two documents: the current one, 'D2.3.1 M-Sec pilots definition, setup and citizen involvement report – 1st version', which contains a detailed update of the initial plan of the pilots, including among others, the work done to involve not only citizens but also stakeholders, such as, stakeholders' identification, recruitment criteria and the specific recruitment actions according to the target audience. In addition, the current deliverable has taken into account feedback from the 1st year review. The second document, 'D2.3.2 M-Sec pilots definition, setup and citizen involvement report – 2nd version', will include the main outcomes, feedback captured and lessons learnt from the 1st trial of the pilots, and it is planned to be submitted by November (M29). In addition, once the 2nd trial of the pilots has been completed and the results analysed, the final version of this report, D2.4, will be submitted.

After an in-depth analysis of the pilots described in D2.2, taking into account that for some of these pilots both their relation to the M-Sec objectives/results as well as their architectural view were similar, the number of pilots has been reduced, without reducing the workload or the scope of the project. Table 3-1 shows a summary of the M-Sec pilots to be implemented in the pilot cities.

Table 3-1: Summary of M-Sec pilots

Pilot(s)	Pilot's names	City
Pilot 1	Secured IoT devices to enrich strolls across smart city parks	Santander
Pilot 2	Home Monitoring Security System for ageing people	Santander
Pilot 3	Secure and Trustworthy Mobile Sensing Platform	Fujisawa
Pilot 4	Secure Affective Participatory Sensing of City Events (cross-border)	Fujisawa & Santander
Pilot 5	Smart City Data Marketplace with secure Multi-layer Technologies	Fujisawa & Santander