



**Multi-layered
Security
Technologies**
for hyper-connected
smart cities

**D2.4: M-Sec pilots definition, setup and
citizen involvement report – Second version**

October 2021



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	D2.4 M-Sec pilots definition, setup and citizen involvement report – 2 nd version
Work Package	WP2
Submission date	October 2021
Deliverable lead	AYTOSAN/NTTE
Authors	TST, WLI, CEA, F6S, AYTOSAN, KEIO, NTTE, YNU, ICCS
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	19 July 2021	Sonia Sotero (AYTOSAN)	ToC
v0.2	27 August 2021	Sonia Sotero (AYTOSAN)	New ToC
v0.3	13 September 2021	Vanessa Clemente (WLI)	Updated Section 2 Pilot 2 Use Case 2
v0.4	14 September 2021	Takehiro Kitano (NTTDMC)	Updated Section Data protection policies on 2.3/2.4/2.5, Section 3
v0.5	14 September 2021	Mathieu Gallissot (CEA)	Updated section 3
v0.6	16 September 2021	Takehiro Kitano (NTTDMC)	Updated Section Data protection policies on 2.3/2.4/2.5 and Section 3
v0.7	20 September 2021	Sonia Sotero (AYTOSAN)	Updated Introduction & Section 2; engagement process & data protection policies on section 2.1
v0.8	21 September 2021	Alberto Puras (TST)	Updated section 2.1 (Technical Approach, Data Management, Pilot Setup and KPIs)
v0.9	22 September 2021	Mari Seki (NTTE)	Updated Section 2.5
v0.10	22 September 2021	Keiko Doguchi (NTTE)	Update section 2.5
v0.11	22 September 2021	Alberto Puras (TST)	Updated section 2.1 (Pilot scenario and objectives). Contributions to section 3
v0.12	22 September 2021	Sonia Sotero (AYTOSAN)	Updated Engagement process on 2.4/2.5 & Data protection policies on 2.4
v0.13	23 September 2021	Vanessa Clemente (WLI)	Updated section 2.2 and section 3
v0.14	23 September 2021	George Palaiokrassas (ICCS)	Updated section 3
v0.15	24 September 2021	Sonia Sotero (AYTOSAN)	Updated section 2.4 Cross border KPIs & questionnaire
v0.16	25 September 2021	Keiko Doguchi (NTTE)	Updated section 2.4
v0.17	25 September 2021	Akira Tsuge (Keio)	Added description of 2.3 and 2.4
v0.18	27 September 2021	George Palaiokrassas (ICCS)	Added content to 2.5
v0.19	28 September 2021	Sonia Sotero (AYTOSAN)	Updated section 2.4 Cross border pilot, section 2.5 & Section 3
v0.20	28 September 2021	Aamir Bokhari (YNU)	Update section 2.3 pilot 3 (UC3)
v0.21	28 September 2021	Mathieu Gallissot (CEA)	Updated section 3
v0.22	29 September 2021	Vanessa Clemente (WLI)	Reviewed document and provide some comments to be addressed
v0.23	29 September 2021	Keiko Doguchi (NTTE)	Updated section 2.5 Data protection policies and processes
v0.24	29 September 2021	George Palaiokrassas (ICCS)	Updated Section 3.1
v0.25	30 September 2021	Keiko Doguchi (NTTE)	Updated section 2.5 Summary
v0.26	30 September 2021	Takehiro Kitano (NTTDMC)	Updated section 2.4
v0.27	30 September 2021	Vanessa Clemente (WLI)	Updated section 2.2 and 3
v0.28	30 September 2021	Alberto Puras (TST)	Updated section 2.1
v0.29	1 October 2021	Sonia Sotero (AYTOSAN)	Updated sections 2.1, 2.4, 2.5, 3.2 & 3.3
v0.30	1 October 2021	Alberto Puras (TST)	Updated section 3.2
v0.31	4 October 2021	Akira Tsuge (Keio)	Updated Final Pilot Results (section 2.4)
v0.32	4 October 2021	Vanessa Clemente (WLI)	Updated section 2.2 Summary Lessons Learned
v0.33	4 October 2021	Sonia Sotero (AYTOSAN)	Merging contributions & conclusions
v0.34	4 October 2021	Takehiro Kitano (NTTDMC)	Updated Section 3.2
v0.35	5 October 2021	Orfeas Voutyras (ICCS)	Internal review





V0.35b	5 October 2021	Kenji Tei (WU)	Added internal review
V0.36	6 October 2021	George Palaiokrassas (ICCS)	Updated section 2.5
V0.37	6 October 2021	George Palaiokrassas (ICCS)	Updated Section 2.5
V0.38	7 October 2021	Sonia Sotero (AYTOSAN)	Updated most internal review comments
V0.39	7 October 2021	Vanessa Clemente (WLI)	Minor format changes
V0.40	7 October 2021	Akira Tsuge (Keio)	Updated most internal review comments
V0.41	8 October 2021	Sonia Sotero (AYTOSAN)	Almost ready
V0.42	11 October 2021	Akira Tsuge (Keio)	Updated Table 3-4
V1.0	13 October 2021	Sonia Sotero (AYTOSAN)	Final version





Table of Contents

Version history.....	3
Table of Contents	5
List of Tables	6
List of Figures.....	8
Glossary	11
1 Introduction	12
1.1 Scope of the document	12
1.2 Relation to other WPs and Tasks.....	12
1.3 Methodology followed	13
2 M-Sec Pilots	14
2.1 Pilot 1 (Use Case 1): Secured IoT devices to enrich strolls across smart city parks	16
2.2 Pilot 2 (Use case 2): Home Monitoring Security System for ageing people.....	31
2.3 Pilot 3 (Use case 3): Secure and Trustworthy Mobile Sensing Platform	55
2.4 Pilot 4 (Use case 4): Secure Affective Participatory Sensing of City Events (crossborder).....	64
2.5 Pilot 5 (Use case 5): Smart City Data Marketplace with secure Multi-layer Technologies	90
3 Common Data Governance and Data Protection Policies	103
3.1 Privacy functions across Functional Groups.....	103
3.2 Privacy-cautions for user interfaces applicability per UC.....	106
4 Conclusions	110
Annex 1 – UC4 representative agreement	111





List of Tables

Table 2-1: M-Sec pilots	14
Table 2-2: Use Case1 Pilot 1 Challenges & Mitigation actions	17
Table 2-3: Use Case1 Pilot 1 data management	21
Table 2-4: Factsheet for Use Case1	23
Table 2-5: Use Case1 setup.....	27
Table 2-6: Use Case 1 Pilot 1 KPIs	27
Table 2-7: Use Case2 Pilot 2 Challenges & Mitigation actions	37
Table 2-8: Use Case2 data management.....	42
Table 2-9: Fact sheet for Use-case 2.....	43
Table 2-10: Use Case2 set up.....	49
Table 2-11: Use Case2 KPIs	49
Table 2-12: Use Case3 Challenges & Mitigation actions.....	56
Table 2-13: Use Case3 Pilot 3 data management	58
Table 2-14: Fact sheet for Use-case 3.....	59
Table 2-15: Use Case3 set up.....	61
Table 2-16: Use Case3 Pilot3 KPIs.....	61
Table 2-17: Use Case4 challenges and mitigations	65
Table 2-18: Actual number of reports by user in PHASE 1	67
Table 2-19: Actual number of reports by user in PHASE 2	69
Table 2-20: Actual number of reports by user in PHASE 3	74
Table 2-21: Use Case4 Pilot 4 data management	77
Table 2-22: Fact sheet for Use-case 4.....	77
Table 2-23: Use Case4 set up.....	84
Table 2-24: Use Case4 Pilot 4 KPIs.....	85
Table 2-25: Detail of sensor data available in M-Sec Marketplace.....	90
Table 2-26: Use Case5 Pilot 5 Challenges & Mitigation actions.	92
Table 2-27: Use Case5 Pilot 5 data management	96
Table 2-28: Fact sheet for Use-case 5.....	97
Table 2-29: Use Case5 set up.....	100





Table 2–30. Use Case 5 Pilot 5 KPIs	100
Table 3–1. GDPR obligations	103
Table 3-2: Use Case1 Fundamental principles	106
Table 3-3: Use Case2 Fundamental principles	107
Table 3-4: Use Case4 Fundamental principles	108





List of Figures

Figure 1—1: Relation of T2.2 to other WPs and Tasks	13
Figure 2—1: Las Llamas park in Santander (Spain).....	17
Figure 2—2: Pilot1: Friend-users in las Llamas park.....	19
Figure 2—3: Pilot1: Screenshots of the piece of news published in local newspapers.....	19
Figure 2—4: Pilot1 information at Santander municipal website.....	20
Figure 2—5: Pilot1 Videos in English & Spanish	21
Figure 2—6: Pilot1 Blogpost and Brochure	21
Figure 2—7: Pilot1 website registration phase: user's credentials.....	22
Figure 2—8: Pilot1 website registration phase: Informed consent	23
Figure 2—9: Architecture of Use Case 1.....	25
Figure 2—10: Prototype of the crow counting PCB (left) and device deployed in Pilot 1 (right)	26
Figure 2—11: Environmental Monitoring devices in Pilot 1 (left) and closer view of the device (right)	26
Figure 2—12: Senior Care Portal	32
Figure 2—13: Senior Care: Dashboard	33
Figure 2—14: Senior Care: User's management	34
Figure 2—15: Senior Care: User's details	35
Figure 2—16: Senior Care: Add New User.....	35
Figure 2—17: Senior Care: Device Management	36
Figure 2—18: Senior Care: Rules Management	37
Figure 2—19: Senior Care: Statistics Module.....	39
Figure 2—20: Senior Care: Comments Module.....	40
Figure 2—21: Senior Care Blogpost and Brochure.....	41
Figure 2—22: Senior Care Video Demo	41
Figure 2—23: Pilot2 information at Santander municipal website and video with Spanish subtitles	42
Figure 2—24: Senior Care Exports User's Data	45
Figure 2—25: Senior Care Deletes User Action.....	45
Figure 2—26: Senior Care and M-Sec interaction Diagram	46
Figure 2—27: Squid Link Gateway Caburn	46
Figure 2—28: Door/Window Opening Sensor Caburn	47





Figure 2—29: Motion Sensor Mini Caburn.....	47
Figure 2—30: Smart Plug Mini Caburn.....	47
Figure 2—31: Eclipse sensiNact Platform.....	48
Figure 2—32: Mobile Sensing by 60 Garbage trucks in Fujisawa city	55
Figure 2—33: Keio mobile sensing platform based on SOXFire as IoT platform for Smart city.....	55
Figure 2—34: M-Sec Secure solutions which is integrated in Keio mobile sensing platform	56
Figure 2—35: Pilot3 Blogpost and Brochure	57
Figure 2—36: Pilot3 Videos in English; Japanese & Spanish	58
Figure 2—37: Architecture of Use Case 3.....	60
Figure 2—38: Use Case 3 detail	60
Figure 2—39: UC4 Overview.....	64
Figure 2—40: Fujisawa Jazz Meetin’ Photos	66
Figure 2—41: M-Sec SmileCityReport Booth and Flyer	66
Figure 2—42: SmileCityReport Themes for Fujisawa Jazz Meetin’	67
Figure 2—43: Results of UC4 Pilot (PHASE 1).....	68
Figure 2—44: SmileCityReport Themes for UC4 pilot PHASE2.....	69
Figure 2—45: Results of UC4 Pilot (PHASE 2).....	70
Figure 2—46: Users’ post from each theme PHASE2.....	71
Figure 2—47: Translation functionality available on the 1 st level (left side), but not on the 2 nd (right side) 72	
Figure 2—48: SmileCityReport Themes for UC4 pilot PHASE3	73
Figure 2—49: Users’ post from “The most beautiful views of my city” theme PHASE3	73
Figure 2—50: Users’ post from “Gastronomic experiences in my city” theme PHASE3	74
Figure 2—51: Results of UC4 Pilot (PHASE 3).....	75
Figure 2—52: Pilot4 Blogpost and Brochure	76
Figure 2—53: Pilot4 Video	76
Figure 2—54: Pilot4 information at Santander municipal website and video with Spanish subtitles	77
Figure 2—55: Informed consent for EU citizens (English version)	81
Figure 2—56: Privacy Policy in Markets: EU side and Japanese side	82
Figure 2—57: Spanish version of the Informed Consent to be accepted before registration phase.....	82
Figure 2—58: Use Case 4 Architecture View.....	83
Figure 2—59: Automatically Privacy Data Protection by GANonymizer	84





Figure 2—60: Japanese & Spanish version of the pop-up questionnaire message.....	85
Figure 2—61: Marketplace Initial User Interface.....	91
Figure 2—62: Marketplace Interface from Smile City Report app and Marketplace Dashboard on Smartphones	93
Figure 2—63: Use Case 5 Blogpost	94
Figure 2—64: Use Case 5 Videos in English & Japanese	94
Figure 2—65: Use Case 5 Brochure	94
Figure 2—66: Pilot5 information at Santander municipal website and video with Spanish subtitles	95
Figure 2—67: New Marketplace User Interface	96
Figure 2—68: Use Case 5 Architecture View	99
Figure 3—1: NIST cybersecurity framework with M-Sec component mapped to each step	105





Glossary

Acronym	Description	Acronym	Description
APPI	Act on the Protection of Personal Information	MQTT	Message Queuing Telemetry Transport
BT	Bluetooth	NoSQL	Not only SQL
D	Deliverable	PM2.5	Particulate Matter 2.5
DDoS	Denial of service	QR code	Quick Response Code
DPIA	Data Privacy Impact Assessment	SCR	Smile City Report
DPO	Data Protection Officer	SQL	Structured Query Language
eCO2	equivalent CO2	SSH	Secure SHell
F2F	face to Face	T	Task
FG	Functional Group	TCP	Transmission Control Protocol
GDPR	General Data Privacy Regulation	ToC	Table of Contents
ICT	Information and Communication Technology	TPM	Trusted Platform Module
ID	Identifier	UC	Use Case
iOS	iPhone Operating System	URL	Uniform Resource Locator
IoT	Internet of Things	UV-A	Ultraviolet A
IP	Internet Protocol	VOC	Volatile Organic Compound
JSON	JavaScript Object Notation	WP	Work Package
KPI	Key Performance Indicator	WiFi	Wireless Fidelity
MAC	Media Access Control	XML	Extensible Markup Language
		XMPP	Extensible Messaging and Presence Protocol





1 Introduction

1.1 Scope of the document

The main purpose of deliverable 'D2.4 M-Sec pilots definition, setup and citizen involvement report – 2nd version' is to provide an assessment of the pilots carried out in both cities, Santander and Fujisawa, within the third year of the M-Sec project.

This report includes in detail the main results of the pilots, such as the level of participation, the feedback captured from participants used as a source of changes, improvements and updates for developments within the technical work packages. In addition, the impact of the pandemic has been analysed, first identifying potential challenges and then applying mitigation actions to adapt the implementation of pilots to the current situation, without undermining the success of the pilots.

In addition, this deliverable takes into consideration feedback from the 2nd year review, addressing the main pilot-related issues. The document follows an iterative approach, whereby the current deliverable is the third report on the M-sec pilots, which completes and updates the information provided in previous deliverables, D2.3.1 and D2.3.2.

1.2 Relation to other WPs and Tasks

'Task 2.2 – M-Sec Pilots: Definition, setup and citizens involvement' is fed by inputs from other WP2 tasks, such as '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 next figure, an iterative approach has been followed which enabled that lessons learnt during the first trial of the pilots have been used as inputs for WP3 as well as 'WP4 – Multi-layered Security Technologies', and as a basis for improvements and updates of developments, with the aim of providing an enhanced and more end-user-oriented solution during the second trial of the pilots.



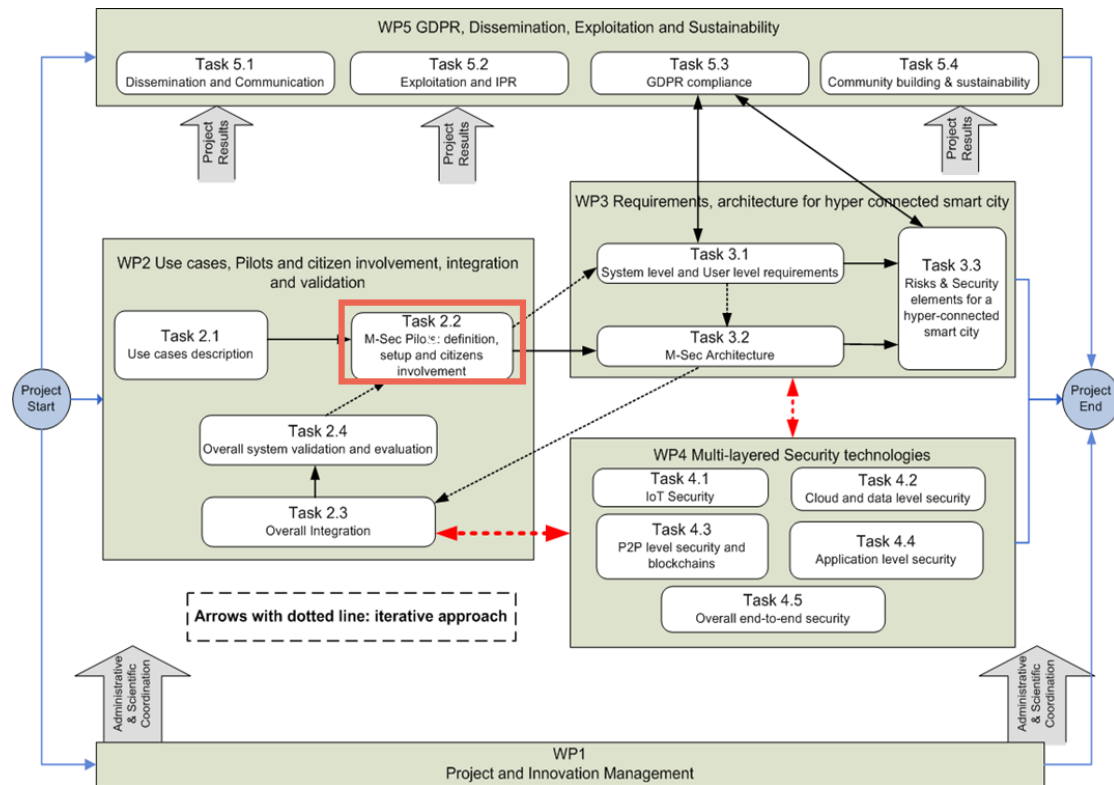


Figure 1—1: Relation of T2.2 to other WPs and Tasks

1.3 Methodology followed

As stated in previous deliverables, the main objective of these pilots is to test and validate the M-Sec architecture and platform in real scenarios, ensuring that technological developments are able to meet cities' needs and allowing M-Sec results to be exploited to develop as well as to offer new smart city applications.

The implementation of the M-Sec pilots follows an iterative approach, including two trials in the case of the pilots conducted individually in each of the M-Sec cities, Santander and Fujisawa, and one trial in the case of the cross-border pilots, carried out in both cities simultaneously.

The iterative approach initially included two deliverables 'D2.3 M-Sec pilots definition, setup and citizen involvement report – 1st version' and 'D2.4 M-Sec pilots definition, setup and citizen involvement report – 2nd version'. Due to the pandemic situation, none of the pilots had started by the delivery date of the first deliverable, so the M-Sec consortium decided to split it into two: D2.3.1, which 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; and D2.3.2, which includes the main outcomes, feedback from end-users and stakeholders as well as lessons learnt from the first trial of the pilots. Finally, the current deliverable provides a detailed report of the pilots carried out in both cities, Santander and Fujisawa, within the third year of the M-Sec project.





2 M-Sec Pilots

This section provides a detailed report of the five pilots that have been conducted, in order to validate the use cases defined in D2.1 and update the plan described in D2.2, in Santander and Fujisawa during the third year of the project. Two pilots have been carried out in Santander, one in Fujisawa and two in both cities simultaneously, the cross-border pilots.

Table 2-1: 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 (cross-border)	Fujisawa & Santander

Considering the uniqueness of the different pilots and the need of homogenising them, a common approach is adopted in the current report. Therefore, for each one of the pilots, the following specific information is provided:

- Pilot scenario and objectives, including a description of the pilot and its re-orientation due to the pandemic situation if applicable.
- Challenges and mitigation actions on pandemic situation, including a list of the main challenges identified together with a description of the actions that have been taken to tackle them.
- Engagement process with citizens and stakeholders, describing how the relationship with participants has been adapted to the pandemic situation, trying to maximise the promotion and visibility of the pilot.
- Data management, providing an update on the Data management reported in D2.3.
- Data protection policies and processes, describing how GDPR and/or APPI compliance has been fulfilled.
- Technical approach – M-Sec components, including the latest version of the architecture of each pilot as well as a description of the security provided by each M-Sec component.





- Pilot setup, providing details such as the number and type of devices deployed, the number of participants, when and how the pilot was launched and carried out.
- KPIs, including the metric indicators defined in D2.3 that will allow checking the success of each pilot.
- Questionnaires, including the surveys circulated among pilot's participants in order to get their feedback.
- Summary – lessons learned, sustainability, highlighting the most relevant outcomes observed during the course of each pilot.





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

Pilot scenario and objectives

Concerns about the impact of the urban environment in individual's behaviour and health have come to the fore and citizens that are subjected to long-term exposures to such kind of environment increasingly demand more information and the implementation of measures to meet air quality guidelines. In this regard, Pilot 1 consists in the deployment of IoT sensors to measure relevant parameters for the wellbeing of the city's inhabitants. These parameters are temperature, humidity, volatile organic compounds (VOC) and CO₂, as well as the level of occupancy of certain areas where citizens usually get together during their free time.

The scenario selected by the M-Sec team for the deployment of Pilot 1 was Las Llamas Park, an 11-hectare urban park located in the city of Santander. It is considered the largest green lung of the city, given the large number of trees and the extension of the green areas. The selected scenario is especially interesting for the Santander Municipality, given the importance of the park for the city, and the data generated by the Pilot will be useful for the analysis of activity in the area and the programming specific actions.

As a complement to the sensors, Las Llamas Park users can find QR codes scattered throughout the pilot site to encourage them to participate in the pilot. The users have access to a web application where data from sensors and interesting facts about the flora and fauna are presented. Furthermore, the website enables users to rate the quality of the data submitted, providing another layer of validation.





Figure 2—1: Las Llamas park in Santander (Spain)

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.

Challenges and mitigation actions on pandemic situation

Table 2-2: Use Case1 Pilot 1 Challenges & Mitigation actions

Number	Challenge	Mitigation Action
1	Covid-19-related mobility restrictions	Facilitate access through the web app to the different menus and measurements
2	Low interest	Get feedback about what could be more attractive to end users and try to apply it
3	Technical issues	1) Quick reaction to potential failures and/or theft of deployed devices. 2) Periodic interaction among partners involved to polish integrations and act over potential issues.
4	Low number of participants	Trigger alternative means of recruitment, even online ones (meetings via Zoom/Teams).
5	Scalability issues	The validation process should trigger the process of performing new deployments in other relevant areas not only of the city of Santander, but also in smaller villages in the region and in relevant mid-size cities nearby (e.g. Gijón, León). Partners in the consortium must find out how to approach them with the solution.
6	Limited scalability due to covid-19	Initially, web users could only access the information about the flora and fauna of the park by visiting it and reading with their mobile phones the QR codes installed in the park. However, due to the pandemic, this information is also accessible via URL from the





Number

Challenge

Mitigation Action

pilot's website, without physically visiting the park.

Engagement process with citizens and stakeholders

Santander city council's strategy for involving citizens and stakeholders in this type of pilots is as follows. Firstly, the municipal services that could benefit from the technological solution used in the pilot are identified and involved. In this particular case, from the beginning of the M-Sec project, several meetings with the heads of the environmental municipal service as well as the parks & gardens municipal service, in charge of Las Llamas park; industrial engineering municipal service, responsible for the connection of devices to the municipal infrastructure, as well as the computing municipal department, in charge of the city council's communications have been held. In addition to collaborating in the definition of the pilot, they have also collaborated in its follow-up: the definition, visualisation, contents and validation of the website; the sensor's locations, aligning the requirements of the project and the needs of the city, as well as, the identification of the users to be involved in the pilot experience. In this sense, and based on previous experiences, the first stage of the pilot is conducted with what we call "friend users": people who have participated in other EU projects' pilots or who have shown their interest in taking part. It is important to mention that sometimes the solutions to be validated through the pilots are not mature or robust enough to be opened to the general public, so it is essential to test them initially with a small group of users, which is worthwhile to obtain their feedback, and then, depending on the results obtained, open it to a wider audience.

Following this approach, once the pilot was up and running from the technical point of view, a first run of the pilot was set up in Las Llamas Park on 16th July 2021 with a group of 15 friend-users including the councillor for the environment, the head and staff from the parks & gardens municipal service, the innovation municipal service staff and Seobird staff, a non-governmental organisation (NGO) that aims to conserve and study birds and their habitats. After a brief introduction to the M-Sec project and the pilot, friend users were invited to register on the website and went around the park reading the QR codes distributed throughout the park and accessing the measurements of the different sensors installed, while evaluating the displayed information. The following pictures illustrate the first visit to las Llamas park with friend users.





Figure 2—2: Pilot1: Friend-users in las Llamas park

The feedback obtained during this visit was very positive: most of the participants agreed that the website is easy to use as well as the content provided is interesting. Although the next step would have been to launch the pilot at city level, due to technical issues related to some of the deployed sensors, the official opening was postponed to 26th August, when the pilot was finally opened to the entire city population.

At this point, the dissemination of the pilot as well as and the end-users engagement have been carried out through different channels:

- A piece of news was published at several local newspapers, both online and in paper versions, inviting citizens to join this pilot experience.



Figure 2—3: Pilot1: Screenshots of the piece of news published in local newspapers

- The Santander municipal website offers a specific section for the M-sec project, providing information about the project and the pilots oriented to end-users including: a detailed description, how to participate, a contact email address and pilot1 video with Spanish subtitles. This can be seen in the next figure and is available [here](#).





Pilotos M-Sec en Santander:

Piloto1: Enriquezca su visita al parque de las Llamas

La idea principal de este piloto consiste en enriquecer la visita al parque de las Llamas a través del despliegue de una serie de sensores, unos códigos QR y una sencilla aplicación web que permita visualizar los datos generados por los dispositivos anteriores.

A lo largo del parque se han instalado unos códigos QR que proporcionan información sobre la flora y la fauna del parque; también se han instalado una serie de sensores medioambientales y cuenta personas que ofrecerán información sobre parámetros tales como la temperatura, humedad, los niveles de CO₂, y una estimación del número de personas que visitan el parque.

A través de una sencilla web, los usuarios registrados podrán acceder a la información anterior mientras disfrutan de su paseo por el parque de las Llamas.

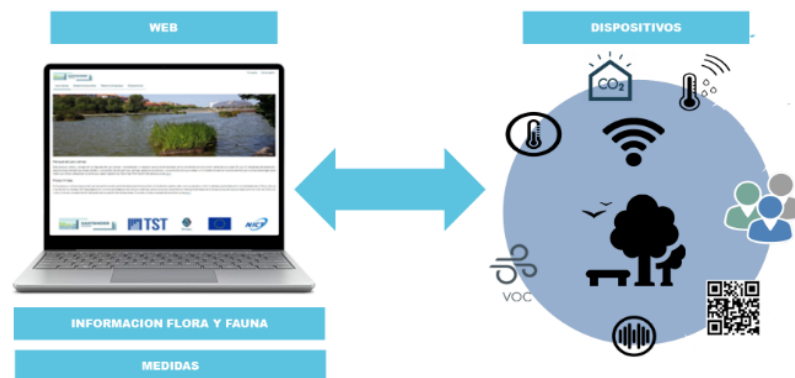


Ilustración del piloto1

La experiencia piloto se puso en marcha a mediados del mes de Julio, con un grupo reducido de usuarios y, actualmente está abierto a todo el público que esté interesado en participar, accediendo a la WEB (<https://msec-santander.com>) o leyendo los códigos QR instalados en el parque.

En este enlace podéis acceder al vídeo del piloto1.

¿Cómo puedo participar?

Si quiere ampliar información en castellano del proyecto y/o los pilotos, contacte con el área de innovación a través del siguiente correo electrónico: innovacion@ayto-santander.es. Estaremos encantados de atenderles.

Si quiere ampliar información sobre el proyecto, visite la web oficial del proyecto (en inglés): www.msecproject.eu donde podrá consultar las Noticias, seguir nuestro trabajo y saber en qué eventos participaremos. Únase a nuestra comunidad en @msecproject y/o M-Sec Project.

Figure 2—4: Pilot1 information at Santander municipal website

- Several consortium dissemination actions have been conducted, such as:
 - Use Case Blogpost where use case1 description is showed, including the main challenges it addresses, the M-Sec approach, the pilot implementation and outcomes together with the value proposition and the business model canvas. Available [here](#).
 - UC Video as a demonstration of the solution and the M-Sec value added. Available [here](#). with English subtitles, and [here](#) with Spanish subtitles.
 - UC Brochure where the unique value proposition is detailed as well as the main stakeholders interested in such a solution, features provided and pilot testimonies. Available [here](#).





Figure 2—5: Pilot1 Videos in English & Spanish

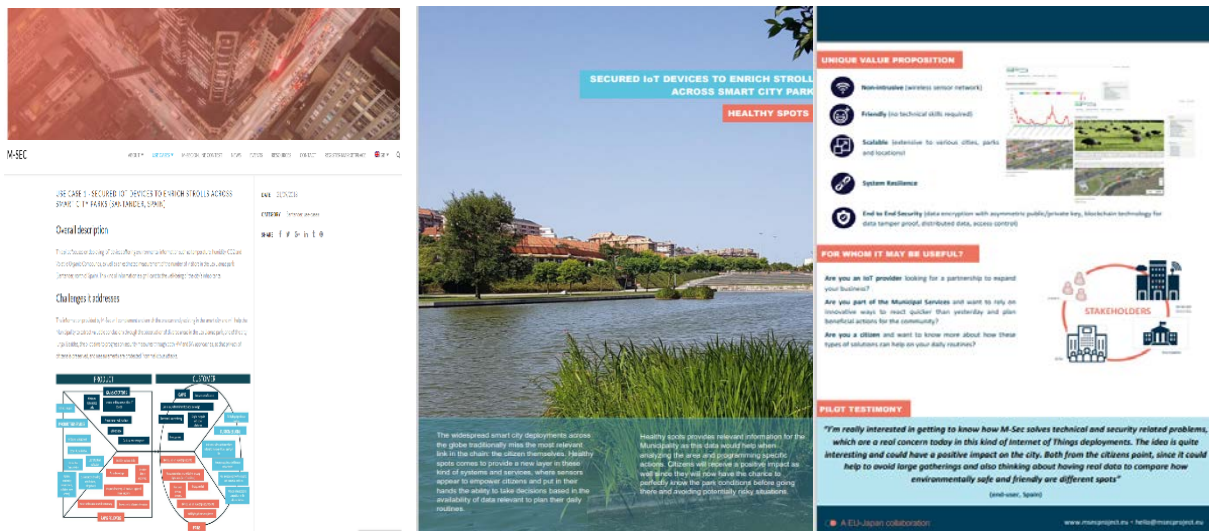


Figure 2—6: Pilot1 Blogpost and Brochure

Data management

Table 2-3: Use Case1 Pilot 1 data management

Type of data	<ul style="list-style-type: none"> Raw data values from environmental sensors (Temperature, humidity, VOC and CO2) The number of devices detected and WiFi MACs provided by the crowd counter
Format of data	<ul style="list-style-type: none"> JSON data exchange format for transporting data within an MQTT connection.
Data collection	<ul style="list-style-type: none"> Measurements are gathered by the IoT devices (environmental sensors and crowd counter), encrypted and sent via Narrow Band-IoT (NB-IoT) communication to a server via TCP. The Park Guide Application access a Data Base through a MySQL connection, while a MQTT connection is used to publish JSON in the corresponding topics, so that data can be forwarded to other M-Sec components.
Data storage	<ul style="list-style-type: none"> Data stored in a NoSQL database (MongoDB) as JSON documents.





Data protection policies and processes

This use case allows the deployment of secured devices in public spaces to collect different types of data. These data include environmental parameters such as temperatures, humidity and carbon dioxide concentration, and also an estimation of the number of visitors in the public space, in las Llamas Park, by monitoring the number of connected devices within a coverage radius using Bluetooth and Wi-Fi network scanning. These data, together with flora and fauna information of the park, accessible through QR codes scattered throughout the pilot side is easily accessible through the website of the pilot, once the user completes the registration phase.

A user is required to register to use the pilot website, and it is at the registration stage when the multi-layer information model is applied, more detailed information about multi-layer information model is included in D5.11, section 5.1. The next figure shows the website registration screen.

The screenshot displays the 'Crear nueva cuenta' (Create new account) page of the Santander Ciudad website. At the top left is the Santander Ciudad logo, and at the top right is a link for 'Iniciar sesión' (Log in). Below the logo, there are three buttons: 'Iniciar sesión', 'Crear nueva cuenta' (which is highlighted), and 'Reinicializar su contraseña' (Reset your password). The main form area is titled 'Crear nueva cuenta' and contains the following fields and instructions:

- Dirección de correo electrónico ***: A text input field. Below it, a note states: 'Una dirección de correo electrónico válida. Todos los correos electrónicos del sistema se enviarán a esa dirección. La dirección de correo electrónico no se hará pública y sólo se utiliza para recibir una nueva contraseña o si quiere recibir ciertas noticias o notificaciones por correo electrónico.'
- Usuario ***: A text input field. Below it, a note states: 'Varios caracteres están permitidos, incluyendo los espacios, puntos (.), guiones (-), comillas ('), guiones bajos (_) y el signo @.'
- Contraseña ***: A password input field. Below it, a strength indicator bar is shown.
- Fortaleza de la contraseña:**: A label for the password strength indicator.
- Confirmar contraseña ***: A second password input field.
- Las contraseñas coinciden:**: A label indicating that the passwords match.
- Proponer una contraseña para la cuenta nueva en ambos campos.**: A note asking the user to provide a password for the new account in both fields.
- ☐ **Acepto las condiciones establecidas en la política de privacidad y el consentimiento informado. ***: A checkbox for accepting terms and conditions. Below it is a link: 'Política de privacidad y Consentimiento.'

At the bottom of the form is a button labeled 'Crear nueva cuenta'.

Figure 2—7: Pilot1 website registration phase: user's credentials

Once the user introduces their email, user name and password, they are given the option to be informed about and give consent for privacy-related issues. By clicking on the link, the first layer of basic information is displayed, where the user will authorize data processing after being informed on the main concepts of data protection, including the controller, the purpose, the legitimacy, the recipients, the rights and the sources, as can be seen in the following figure. Additionally, a web link is provided that leads to the second layer with additional information, where more detailed information is available.





Iniciar sesión

CONSENTIMIENTO INFORMADO

AUTORIZO al Ayuntamiento de Santander para el tratamiento de mis datos en el marco del programa europeo-japonés M-Sec y sobre la base de la siguiente información proporcionada:

INFORMACIÓN BÁSICA SOBRE LA PROTECCIÓN DE SUS DATOS

Corresponsables	Ayuntamiento de Santander y TST
Finalidad	Participar en el piloto "Enriqueciendo los paseos por los parques de la ciudad mediante dispositivos IoT seguros" ("Secured IoT devices to enrich stroll across smart city parks?"), perteneciente al Proyecto Europeo M-Sec.
Legitimación	Consentimiento del interesado y Misión en Interés Público
Destinatarios	No está prevista la comunicación de datos a terceros.
Derechos	Acceso, rectificación, supresión, oposición, limitación del tratamiento y, en su caso, oposición y portabilidad de los datos.
Procedencia	Los proporcionados por los participantes en el proceso de registro y uso de la app.

Para información adicional relativa a la protección de sus datos, por favor, consulte el siguiente enlace web: <http://santander.es/ayuntamiento/proteccion-datos/informacion-adicional-proteccion-datos>



Figure 2—8: Pilot1 website registration phase: Informed consent

Only when the user accepts the basic information, they can complete their registration and access the website. Below the factsheet on which type of data has been processed is shown.

Table 2-4: Factsheet for Use Case1

Data in encrypted database	Personal data needed at the registry phase in the related app (e-mail + password). Additionally, raw data generated by the sensors.		
Data in blockchain	<ul style="list-style-type: none">Statistically processed environment dataProtect IoT devices by limiting the number of requests that can be made to know the data it collects.		
Does it involve personal data processing?	Yes	Please, specify which kind of data	User ID (e-mail address + password) BT/Wi-Fi MAC addresses from mobile phones detected





Data processing	The purpose of collecting private data in this use case is to actively involve users in the experience the pilot aims to test, evaluating the real usefulness of the data offered by secured IoT sensors developed within the context of M-Sec, complementary to the one already provided by fixed signs in the park. 1. Identification data: <ul style="list-style-type: none">- Details: E-mail address, password- Justification: Necessary for creating the profile and communicate when updates are available.- Minimization controls: No. 2. Connection Data: <ul style="list-style-type: none">- Details: Events logs (technical logs).- Justification: Required for maintenance purposes.- Minimization controls: No.				
Data retention	One month after the finalization of the pilot phase.				
In case, there is personal data, please add the following details:					
DPO	AYTOSAN protecciondedatos@santander.es TST	Controller	TST/AYTOSAN	Processor	TST

Additionally, a joint controller agreement between Santander city council and TST was signed before launching the pilot.

Technical approach – M-Sec components

Pilot 1 is based on two different IoT devices which were developed within the project and their integration with several components of the M-Sec framework (in Deliverable 3.4 a more detailed explanation can be found). The following figure shows the architecture of defined for Pilot 1.

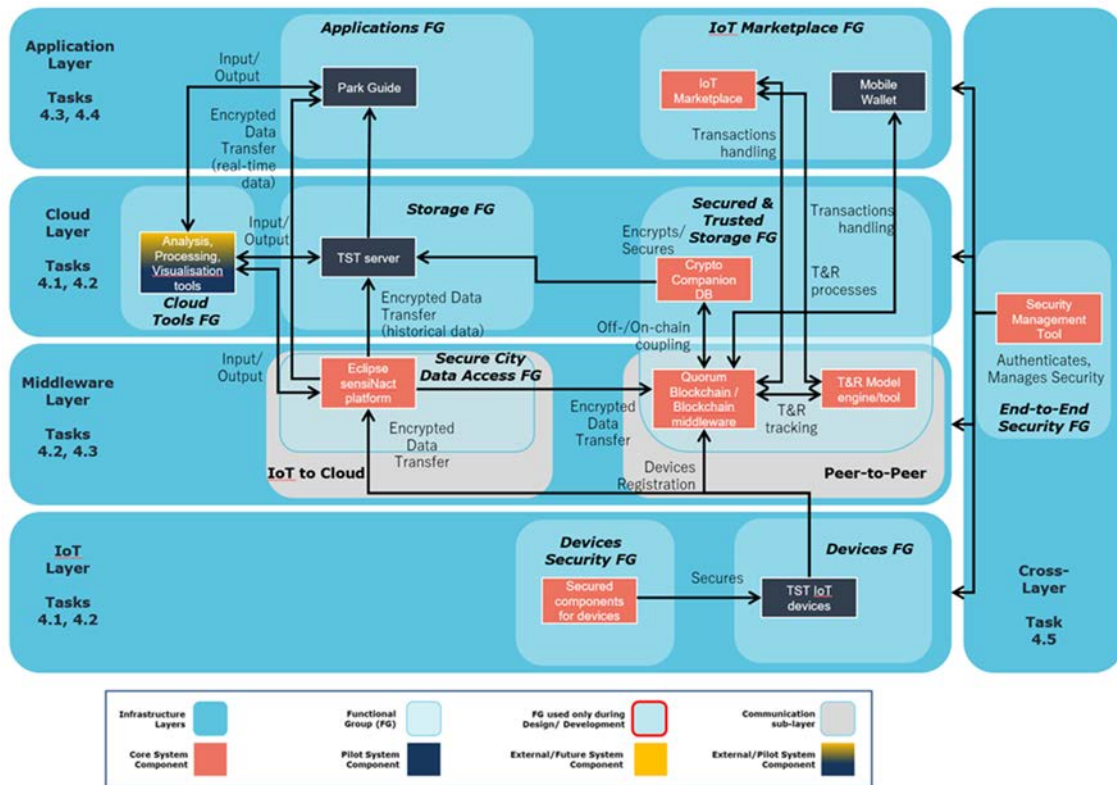


Figure 2—9: Architecture of Use Case 1

Under the M-Sec framework the data collected by the IoT devices are sent to different components:

- The Eclipse sensiNact Platform receives the data through an MQTT connection. There, sensiNact users can visualize the devices and the data and establish their very own analysis.
- The Crypto Companion Database (CCDB) encrypts the data with an asymmetric public/private key pair. Data can only be accessed by the owner who has to be authenticated, and the authorised operators allowed by that owner. At the same time, a hash is generated from all the encrypted data and stored in the Quorum blockchain for data tamper proof.
- The marketplace makes all the data available for the public because it doesn't contain any personal data related to the end user. In the marketplace stakeholders who may be interested on getting this kind of environmental and number of visitors data can buy it using the so-called M-Sec Tokens, which is a cryptocurrency in the form of a smart contract running on blockchain.

One of the IoT devices developed by TST is the so-called crowd counter, and it is intended for detecting visitors through the identification of active Wi-Fi and Bluetooth communications in their smartphones. This way the crowd counter obtains WiFi and Bluetooth MAC addresses of visitors' smartphones and provides an estimation of the number of people in the surroundings of that specific spot. This device is installed in one of the hot spots of the Las Llamas Park, just in the level below its restaurant. The following figure shows the deployed device.

This IoT device includes novel security hardware mechanisms to increase the security level of these physical objects. The implemented mechanism is based on a hardware extension known as "TPM" (Trusted Platform Module) and is used to ensure that security critical information as private keys has not been extracted.





Besides, the developed device implements advanced encryption mechanisms to prevent undesired external accesses that may affect the device functioning and thus the data it delivers.



Figure 2—10: Prototype of the crow counting PCB (left) and device deployed in Pilot 1 (right)

The other kind of devices is in charge of performing environmental monitoring by measuring temperature, humidity, CO₂ and VOC. Five devices were deployed in Las Llamas Park covering a complete longitudinal section of the park, going from one side, closer to the University of Cantabria, to the opposite side, just next to a residential area and crossing the city motorway which separates this housing zone from the park. The following figure shows one environmental sensor installed in the park and a view of the developed hardware with its battery.

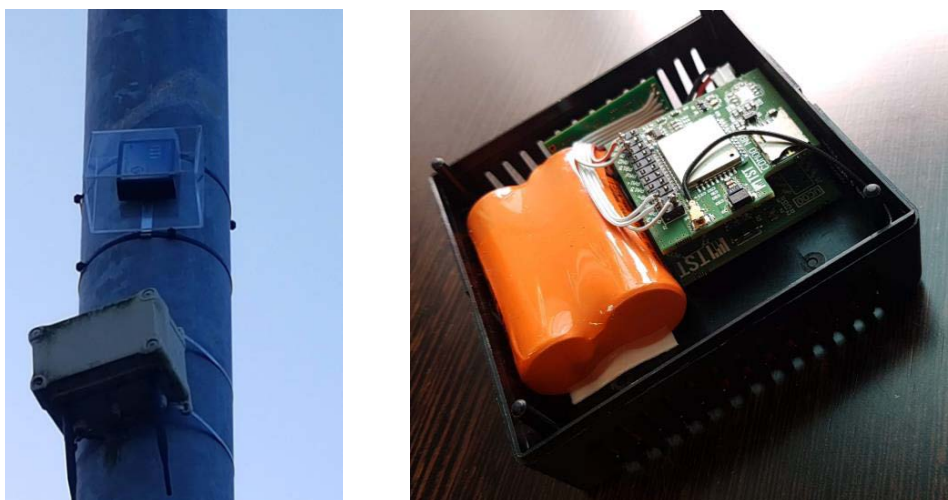


Figure 2—11: Environmental Monitoring devices in Pilot 1 (left) and closer view of the device (right)





From the security point of view, this device includes encryption mechanisms provided by the selected microprocessor from the ST Microelectronics: STM32-L422cbu6 Series.

Pilot setup

A summary of the setup of pilot 1 is shown in the following table.

Table 2-5: Use Case1 setup

Planning	<ul style="list-style-type: none">• Start Date: M26 (September 2020)• Duration: M26 – M39 (15 months)• Phases:<ul style="list-style-type: none">○ PHASE 1 – Design of the Pilot (M26-M27):○ PHASE 2 – Deployment of IoT devices (M27): Sensors installation and connectivity tests.○ PHASE 3 – 1st Trial of the pilot (M27-M37): Integration with the M-Sec platform and refinement of components and Park Guide web.○ PHASE 4 – 2nd Trial of the pilot (M37): Trial with 15 friend users in Las Llamas Park.○ PHASE 5 – Pilot Evaluation (M38-M39): Questionnaires. KPIs follow-up report.
-----------------	---

KPIs

Table 2–6. Use Case 1 Pilot 1 KPIs

#KPI	Goal	How to measure?	Target	How to measure?
#Participants	Minimum number of end users to test the solution provided	Number of end users registered into the system	≥50 users (1 st trial: 10-15 friend users, 2 nd trial: 50 participants)	Number of end users registered into the system
#Active users	To evaluate the real activity of registered participants	Connections to the web app	≥50	Connections to the web app
#Data tampered	Verify data reliability (data has not been modified)	Use Blockchain, sensitive data from this use case can be tamper proof. Data will be modified on purpose during lab testing.	0	Use Blockchain, sensitive data from this use case can be tamper proof. Data will be modified on purpose during lab testing.
#Unauthorised intents to access to data	Avoid unauthorised users have access to sensitive data	Through smart contracts, it is possible to verify whether someone	0	Through smart contracts, it is possible to verify whether someone





#KPI	Goal	How to measure?	Target	How to measure?
		has authorization or not. Warning logs will be received to alert about it.		has authorization or not. Warning logs will be received to alert about it.
#DDoS attacks	Avoid attempts to disrupt normal traffic	Putting IoT devices on the Internet before going public and evaluating their interactions.	0	Putting IoT devices on the Internet before going public and evaluating their interactions.
#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	Attacks to the IoT devices to get information (not available) and/or access to other elements in the system.

Questionnaires

Within the Pilot 1 a questionnaire was prepared to get feedback from users. This questionnaire was implemented through the Google Form service and is detailed below:

User data:

- E-mail
- Profile:
 - o Citizen
 - o Researcher
 - o Technician/developer
 - o Public worker
- Do you have previous experience using IoT devices or Smart City applications?
 - o Yes
 - o No
- Are you aware of the data gathered by the use case and how this affects your privacy?
 - o Yes
 - o No

**From the security point of view, how important are the following aspects
(1 = not important – 5 very important)**

1	2	3	4	5
---	---	---	---	---





To encrypt the data within the device before sending it					
To protect IoT devices from hacking?					
Regarding the Park Guide web....	1	2	3	4	5
Do you like the web? Is it user-friendly? (1 = I do not like it at all – 5 = I like it very much)					
How often do you think you will use the web? (1 = never again – 5 = very often)					
In your opinion, are the provided measurements interesting (1 = not important – 5 very important)	1	2	3	4	5
Temperature					
Humidity					
CO2					
VOC (Volatile Organic Compounds)					
Flora and Fauna					
Number of visitors					
<ul style="list-style-type: none">- Which other parameters you would like to see monitored?- Would you recommend it to other users? Why?					

Summary – lessons learned, sustainability

The main lesson learnt has to do with the reliability/accuracy of the measurements provided by the low-cost sensors integrated within the prototype. In this regard, there was a concern about the accuracy of the provided measurements since low-cost sensors are less reliable compared to the high-end sensors used by meteorological services commonly used by citizens. For this reason, a further effort should be made to ensure the validity of the measured data through their calibration and the implementation of error compensation mechanisms.

In conclusion, the sustainability of the pilot will require the industrialization of the developed prototypes to ensure the reliability of the data provided.





From the end-users' point of view, they liked the experience of walking around the park reading the QR codes, especially those who went with children.





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

Pilot scenario and objectives

The rapid increase in the population in recent years, caused by the increase in life expectancy due to medical, social and economic advances, the lack of close family ties, the result of living alone, together with the increase in the demand for social services and the risks generated by the COVID-19 crisis, make it necessary to rethink innovative solutions and services, as well as find complementary or alternative models to the current ones.

Globally, life expectancy has increased by more than 6 years between 2000 and 2019. In fact, the population of many of the richest countries in the world has life expectancies of over 80 years. In 2019 the life expectancy in Spain, Switzerland, Italy, and Australia was over 83 years. In Japan, it was the highest with close to 85 years¹.

However, older adults are also disproportionately affected by chronic conditions, such as diabetes, arthritis, and heart disease. According to the Centers for Disease Control and Prevention, approximately 85% of older adults have at least one chronic health condition, and 60% have at least two chronic conditions².

In addition, it should be considered the effects and the impact caused by COVID-19 on their lifestyle and wellbeing. Although all groups are at risk of contracting COVID-19, older people is one of the most vulnerable segment facing significant risk of developing severe illness if they contract the disease due to physiological changes that come with ageing and potential underlying health conditions. In addition, the pandemic has occasioned a decrease in social life and fewer in-person social interactions associated with reduced quality of life and increased depression. Difficulties accessing services, sleep disturbances, and a reduction of physical activity were also noted.

The life expectancy growth and, as a consequence, the increase in the demand for public social services makes it necessary to adapt quickly the system to provide solutions to keep the older population safe. If we consider Spain, for the eight million people over 65 years of age, the available places with public coverage in nursing homes (either public or subsidized in private centers) cover only sixty out of every one hundred users. The remaining places are in private centers and without public funding³.

It is clear that the pandemic has accelerated the rise of digital health, a broad concept that includes solutions for telemedicine and teleconsultation, remote monitoring, connected devices, digital health platforms and health apps, among other reasons, to respond to the deficient follow-up that is carried out today to the patient in person. The optimization of resources and the desaturation of the health system goes through the transfer of primary care to the home itself and the improvement in communication with the patient with the passage of the relationship from the physical to the virtual. The new paradigm of the connected patient puts the patient at the center of the experience and in improving their quality of life through regular monitoring of their well-being and health.

Worldline in this line, proposes Senior Care. Senior Care is an IoT platform for home sensors (movement, door and window opening, bed occupancy, smoke detection, electrical activity detection in appliances, etc.) that

¹ [Life Expectancy - Our World in Data](#)

² [Supporting Older Patients with Chronic Conditions | National Institute on Aging \(nih.gov\)](#)

³ [El negocio de las residencias de mayores en España \(infolibre.es\)](#)





enables remote monitoring of the daily activity of older people who live alone. The solution allows the configuration of alarms based on data generated by one sensor, or a combination of several sensors, to alert users to any concerns regarding the security or well-being of elderly people living alone. The solution aims to guarantee the security and safety of people who may be at risk due to factors of age, frailty, loneliness, or dependence.

The Senior Care solution provides discrete, non-intrusive (wireless sensor network) and user-friendly (no technical skills required) support for dependant older people wishing to live a more independent life with privacy and dignity.

The rules configuration feature can be used to set-up different red-flag situations related to daily routines at home that may lead to a serious wellbeing problem for older people living alone. These use cases may be related to their daily routines (activity), their presence in spaces around the home (movement) and their own safety.

Senior Care Assistance provides the following main features:

- 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)

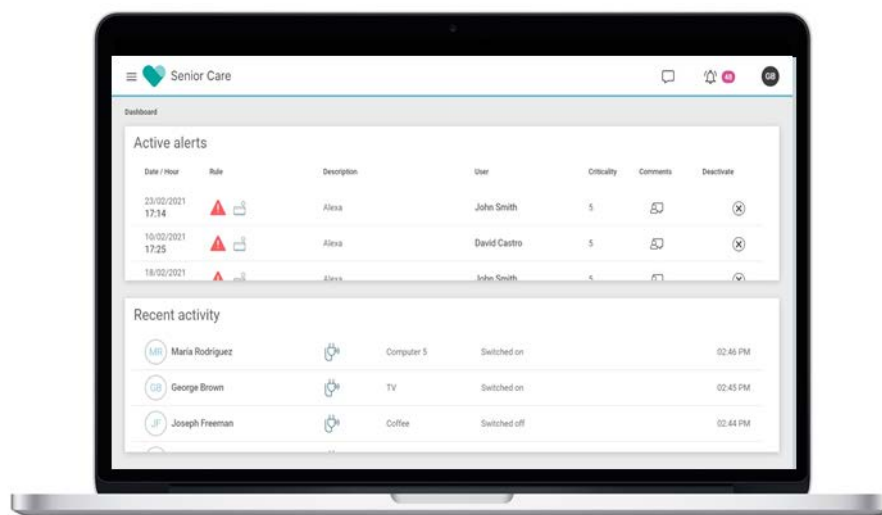


Figure 2—12: Senior Care Portal

The main goals designed for the system (Senior Care + M-Sec platform) that are being tested during the execution of the pilot are:

- Improvement of quality of life of elderly people who live alone.
- 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 tools and sensors.





- 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 Senior 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.

Below we include some screenshots to show the main platform functionalities provided in order to monitor ageing people at their homes through the use of home sensors.

Live Dashboard

Main home page of the platform. From the Dashboard, it is possible to visualize the alerts and the recent activity of each User.

- Header: unread messages, active alerts and settings.
- Alerts:
 - Active alerts are displayed and deactivated.
 - It is possible to access the comments of the users who have active alerts.
- Recent activity: The last events (time and activity) of all senior users of the system.

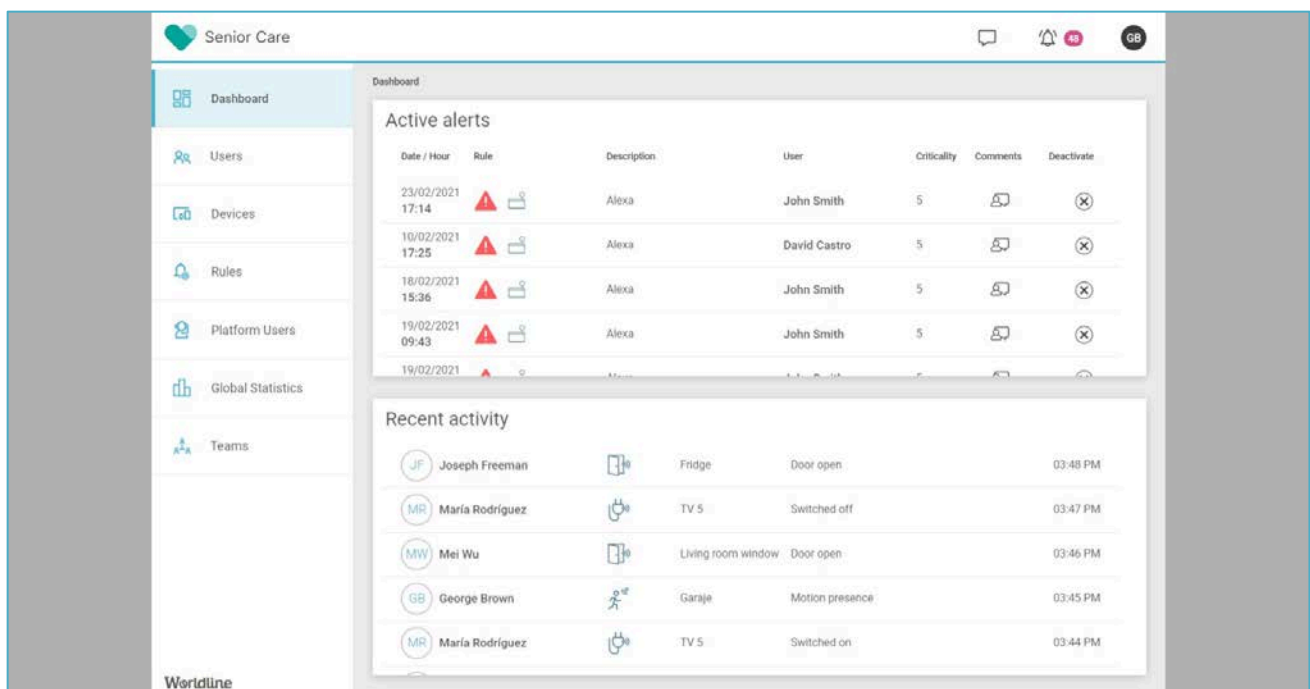


Figure 2—13: Senior Care: Dashboard





Patient/ User Management

This screen provides an overview of all existing Senior Care users (with their basic information).

- Users can be filtered:
 - Active alerts: users with alerts existing
 - Comments: users with comments
 - Status: status of the user at that moment (Active, Paused, Not started, Any, Off)
 - Activity: can be filtered by the date of the last activity. For example, if we select 24h the users on which there are new notifications in the last 24 hours.

It is important to note that there is a drop-down in the users who have active alerts (Red triangle of exclamation mark), which is used to indicate that new alerts exist.

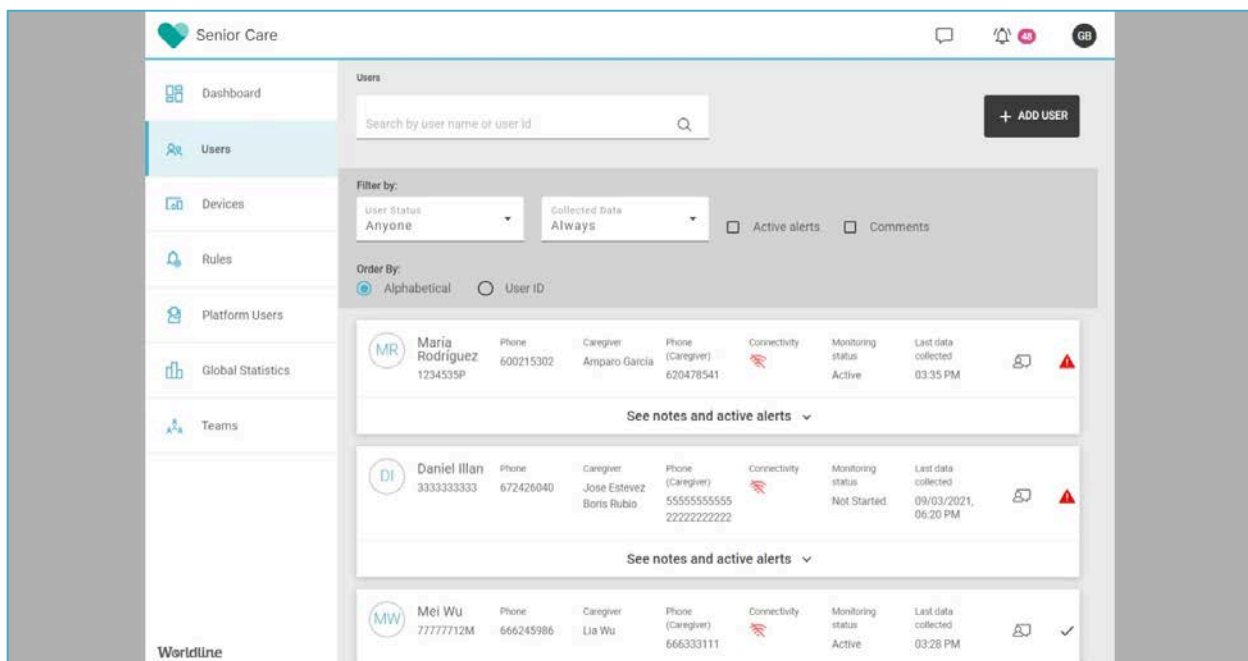


Figure 2—14: Senior Care: User's management

- User's details:
 - Rules tab: tab that leads to a screen which shows the rules that are being applied to that user
 - Devices tab: tab that leads to a screen showing Devices in use for that user
 - Activity tab: tab that shows the User Device activity
 - Contact Details tab: tab that allows to check and modify user profile data such as address, phone, email, etc.



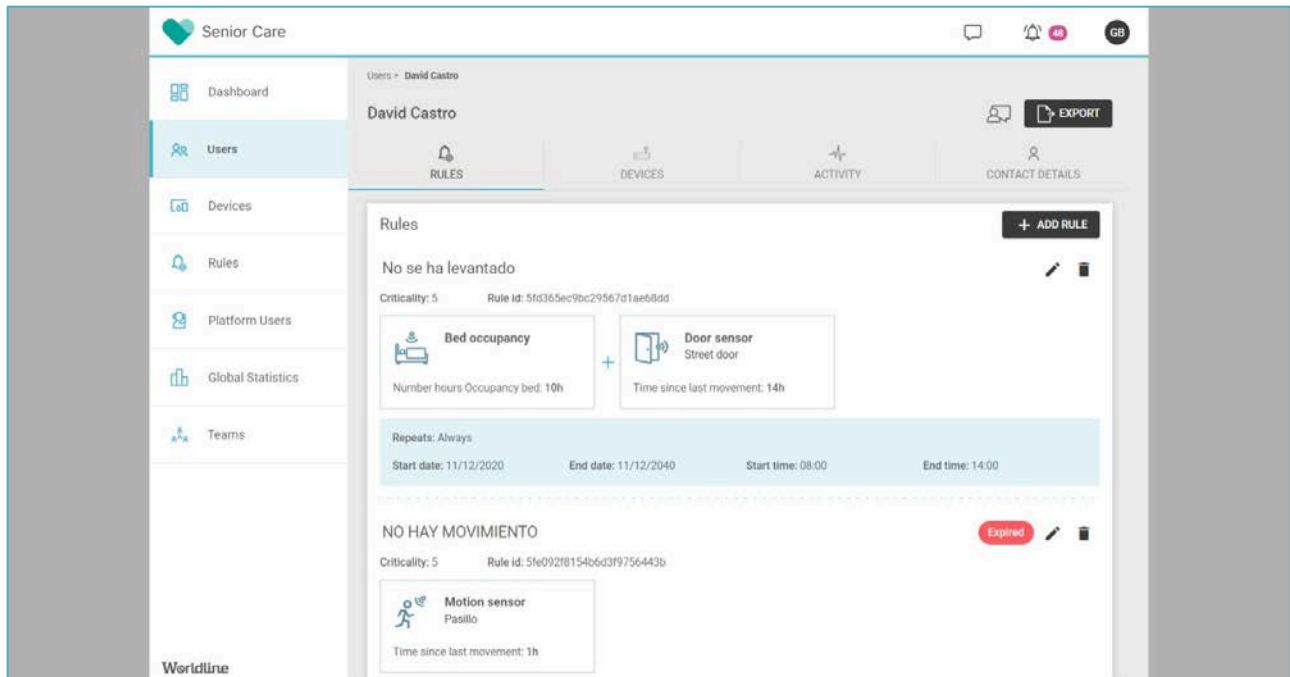


Figure 2—15: Senior Care: User's details

- Users can also be created: Once a new user is created, the user will be subsequently monitored through the system and it will be possible to assign Tele-operators and Managers. The user has to give his consent to the company of Senior Care. There's a field to specify if this consent has been provided.

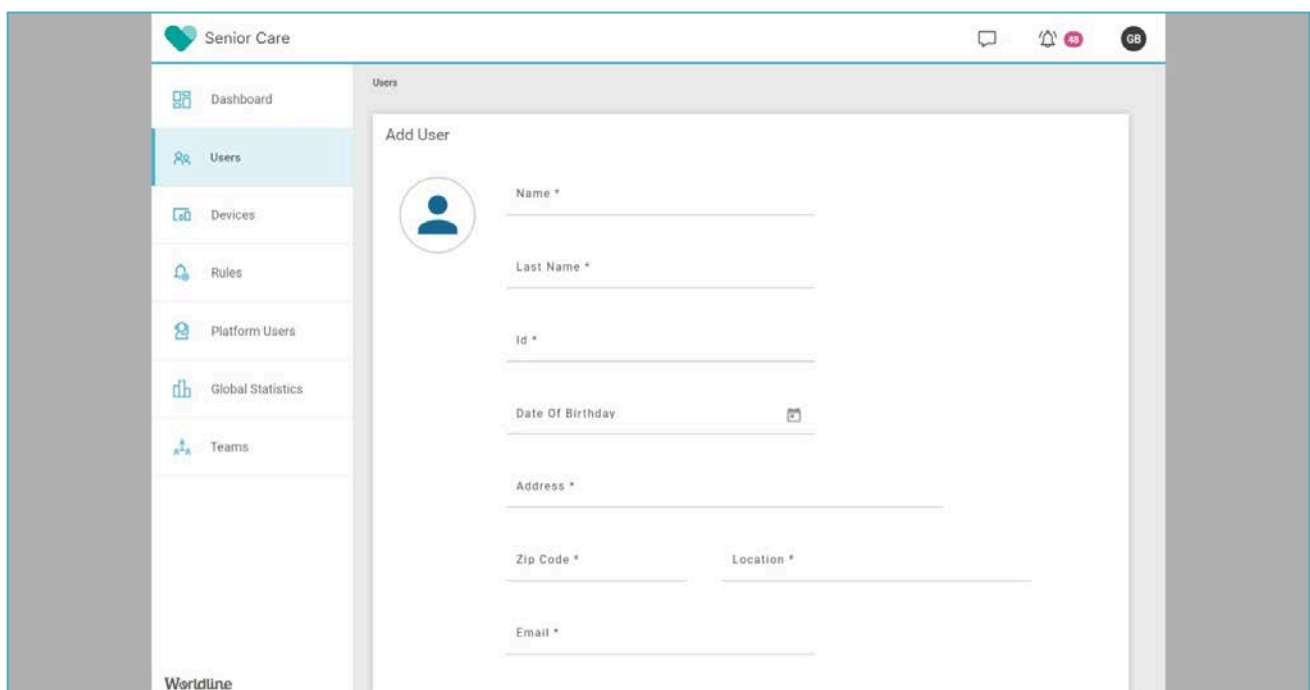


Figure 2—16: Senior Care: Add New User





Device Management

Screen with the data of all the Devices of the system. The history icon leads to the user's Device Activity in question showing this activity exclusively from the selected device (if we select a Gateway: all Devices on that Gateway. if we select a Device: only that Device). When searching for a device, we filter out all fields at the same time.

Alert	Device ID	Type of device	Location	Assigned	Connectivity	Battery
	ALEXA_ID	Alexa	ALEXA_LOCATION1	Peter Gregory		
	1301000100011AA8	Gateway	---	Peter Gregory		
	0200000100011AA8	Gateway	---	John Smith		
	0201000100011AA8	Smoke sensor	Kitchen	John Smith		
	0202000100011AA8	Mattress sensor	Bed	John Smith		
	0203000100011AA8	Door sensor	Fridge	John Smith		
	0204000100011AA8	Smart plug	Nespresso	John Smith		
	0205000100011AA8	Smart plug	TV 2	John Smith		
	0206000100011AA8	Motion sensor	Bathroom 2	John Smith		
	03010001DD11DD66	Alexa	Kitchen	John Smith		

Figure 2—17: Senior Care: Device Management

Alerts & Configuration

Screen to consult and create rules. The rules are algorithms which, depending on the data collected from the devices, generate alerts.



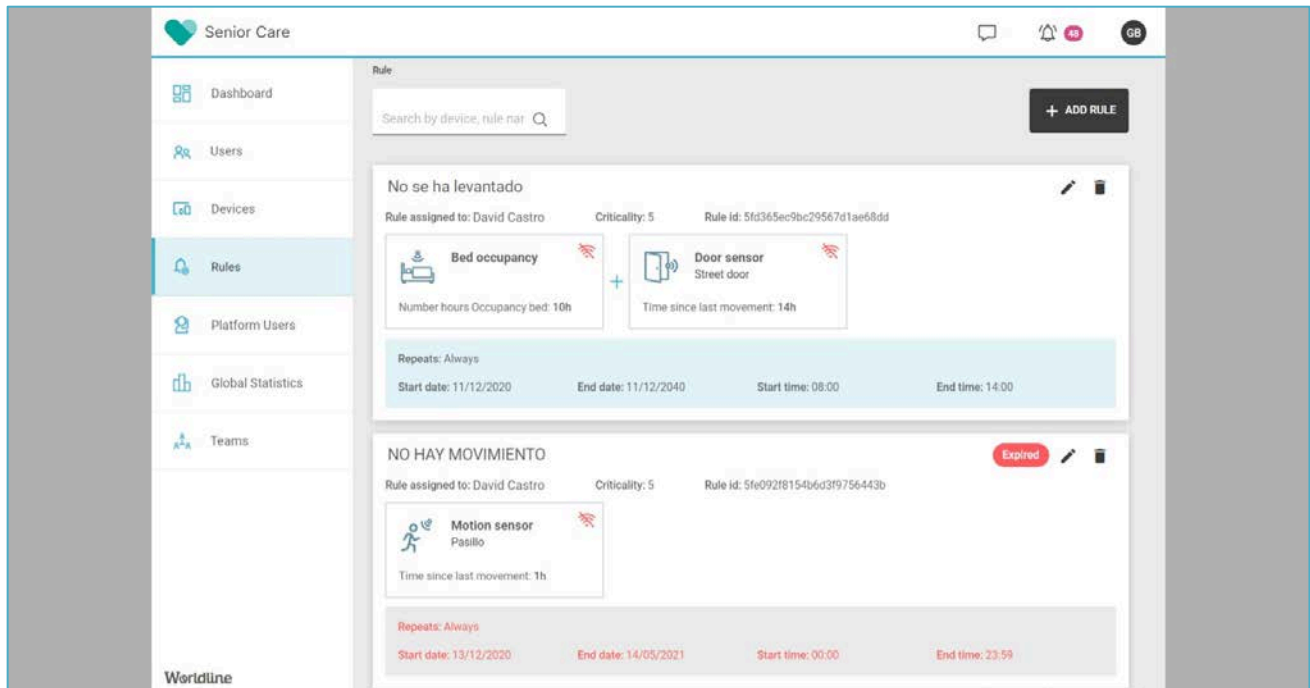


Figure 2—18: Senior Care: Rules Management

Challenges and mitigation actions on pandemic situation

Table 2-7: Use Case2 Pilot 2 Challenges & Mitigation actions

Number	Challenge	Mitigation Action
1	The pilot does not acquire the agreed number of participants.	The consortium has preselected 10 additional users to cover a participant from the pilot eventually.
2	Teleoperators do not have enough time to use/test Senior Care as a parallel system to their current analogic solution	The tele-assistance company has involved several staff members in this pilot therefore, they are able to coordinate to do their daily work and at the same time attend to the Senior Care platform
3	Participants (end-users and tele-assistance provider) are frustrated when technical problems occur with the prototypes.	The solution, along with the integrated M-Sec components, has been tested internally before going on production. Additionally, communication channels, such as email or telephone, have been defined to contact in case of any issue or bug report.
4	Leaks of personal data may lead to lose the confident/trust from end users	M-Sec components integrated within the solution 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.





Number	Challenge	Mitigation Action
5	Risks of a new wave of Covid may lead to restrict visits from the teleassistance party to the user's home. If for example a device is not working properly and needs to be replaced the visit may not be possible...	A protocol is applied to guarantee the tele-assistance service is following the guidelines established by the responsible official authority, restricting home visits to exceptional situations where the person's life is in danger.
6	Delay on the M-Sec integration components	Pilots started running from September 2020 in order to go for an iterative approach adding new functionalities and M-Sec components in an agile way.
7	Devices/solution is not working properly and data is not being reported correctly	Each day the tele-assistance provider verifies with the user status through a short call. All the alarms received are verified in addition with users.
8	Lack of scalability due to Covid-19	This pilot is being tested within a closed environment of participants due to the high cost of the sensor's home kit being provided to each end user. COVID-19 has not caused any impact on the total number of participants.

Engagement process with citizens and stakeholders

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:

From the beginning of the project, a series of F2F and online meetings have taken place involving a) Worldline as technological partner providing the solution, b) Santander City Council easing the implementation in the city, and c) the current tele-assistance provider, Atenzia, the one testing the solution in their infrastructure. Meetings have been held to align the municipal and project needs. Both Municipal Social Services and Atenzia 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. In addition, training sessions have been conducted to show to the tele-assistance operators the use of Senior Care as well as the benefits obtained through M-Sec.

For the pilot phase, contacts for the technical support have been established to facilitate the reporting of bugs or the transfer of any other output related to the pilot testing (i.e. new needs identified). Furthermore, on a weekly base, Atenzia sends Worldline a report with the major events or findings around the platform and its use.

Moreover, one workshop took place just one month after the initiation of the first pilot phase, oriented to exchanging feedback on how the tool has worked so far (positive and negative things, things that are missing, etc.). One of the things developed during the third year of the project and based on the feedback received by Atenzia, has been the implementation of a statistics module as it can be seen below:



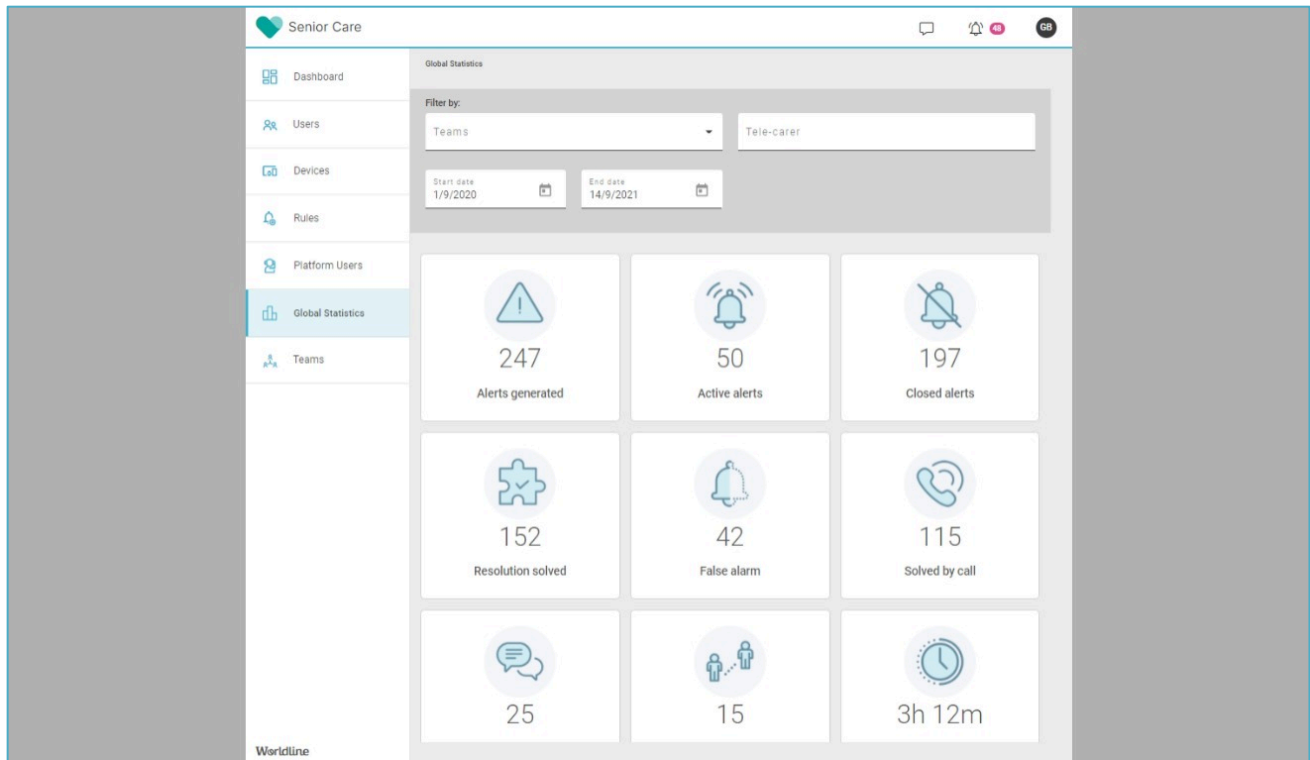


Figure 2—19: Senior Care: Statistics Module

In this screen all the general statistics appear, being able to be filtered by:

- Team
- Tele-operator
- Start date / End date. By default it always appears TODAY.

The following KPIs are included within the statistics module:

- Alert generated: total number of alerts that have been triggered
- Active alerts: alerts currently active
- Closed alerts: number of closed alerts (solved + false alarms)
- Alerts by criticality: alerts distributed by number of criticality
- Fixed alerts: number of fixed alerts
- Total amount of data: size of data collected from users
- False Alarm: number of alerts that have turned out to be system error or alarms that have been triggered erroneously
- Number of events: number of interactions with the system
- Solved by call: alerts contacted by call
- Resolved by message: alerts contacted by message
- Solved by visit: alerts contacted by visit
- Resolution time





In addition, on the workshop conducted during year 2, Atenzia wished a section to add comments for follow-up purposes. The following figure shows the new "Add new comment" section on a test user, named Maria Rodriguez. In the case of a real user of this pilot, their personal data would be anonymised.

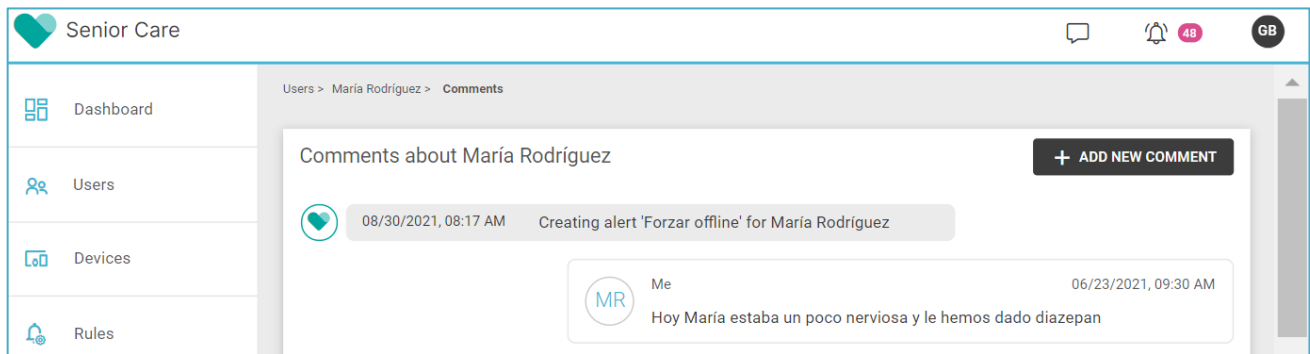


Figure 2—20: Senior Care: Comments Module

Regarding end users, Atenzia counts 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 2020 taking advantage of the regular visits to their homes. During these individual visits, the pilot was explained to each one of the 15 tele-assistance service users, taking into account their profile and circumstances, with the aim of assessing their degree of interest in taking part in the pilot. For pilot purposes, only 5 of the total 15 users were finally selected to test the solution. One of the main advantages of this type of solution for remote monitoring is that it does not present any complexity from the end-user side in terms of installing devices or configuring them which definitely facilitates the user experience considering that the ICT knowledge on the ageing segment is not advanced at all.

During the second week of September 2020, some employees from the tele-assistance party went to the five homes where they installed the devices and the service was explained to them in more detail and the informed consent was provided. Each of the chosen users has different habits. That way, it was possible to place the devices and configure the alarms in a more personalized way. For example, in some cases the bed sensor was placed on the sofa where elderlies watch TV, as the mattress was too thick and did not detect movement. On the other hand, the door opening sensors were mostly installed in the refrigerator with the exception of one user, who gave problems, due to the distance in which it could be placed and therefore it finally was put in the drawer where the user had the medicine.

Pilot dissemination for replication purposes has been done in parallel since the initiation of the pilot in September 2020. Some of the actions conducted are:

- Use Case Blogpost where use case description is shown, including the challenge it addresses, the M-Sec specific approach, the pilot implementation and results as well as the value proposition and the business model canvas. Available [here](#).
- UC Brochure where the unique value proposition is detailed as well as the main stakeholders interested on such a solution, features provided and pilot testimonies. Available [here](#).
- UC Video as a demonstration of the solution and the M-Sec value added. Available [here](#).





Figure 2—21: Senior Care Blogpost and Brochure

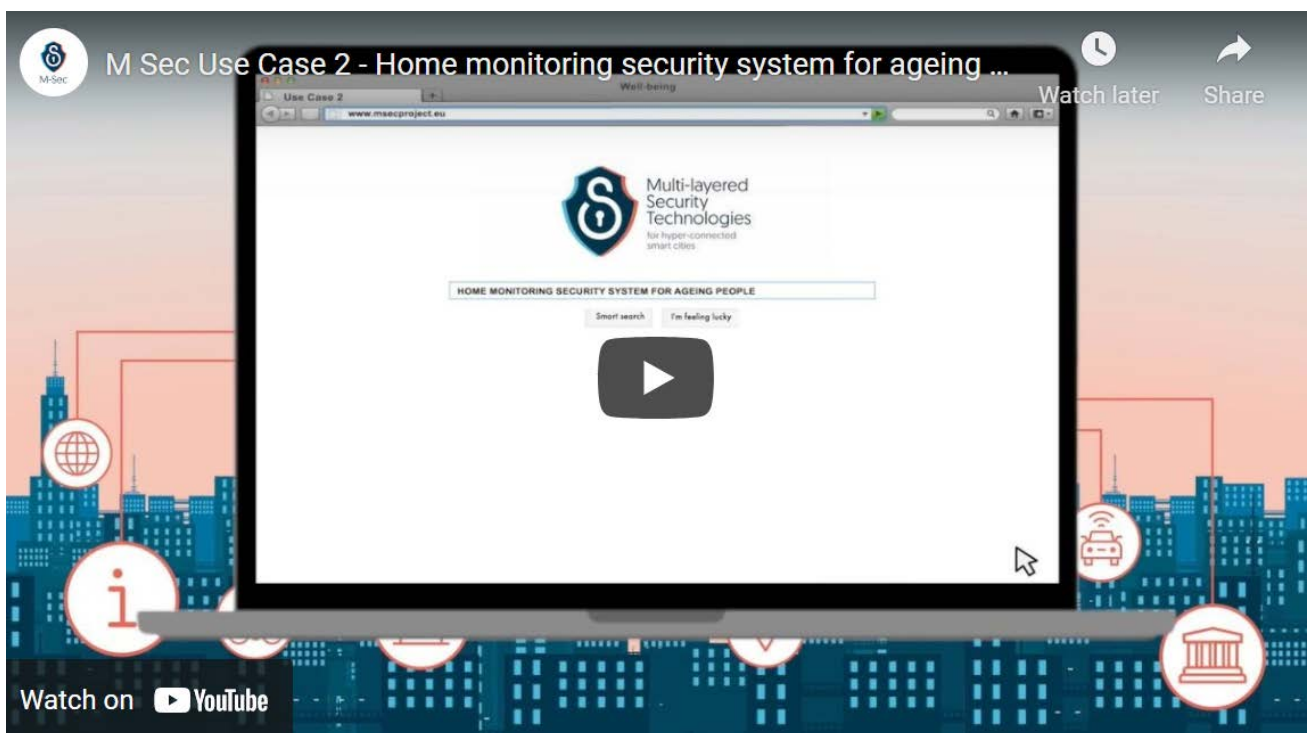


Figure 2—22: Senior Care Video Demo

As mentioned in the previous pilot, Santander municipal website offers a specific section for the M-Sec project, providing information about the project and the pilots oriented to end-users including: a detailed pilot description as well as a pilot2 video with Spanish subtitles. This can be seen in [Figure 2—23](#) and it is available [here](#).





SANTANDER CIUDAD

Buscador Ciudad Servicios al ciudadano Servicios para empresas Ayuntamiento Sede Electrónica

Piloto2: Monitorización de la actividad en el hogar de las personas mayores

Este piloto tiene como objetivo la mejora en la calidad de vida de aquellas personas que pueden estar en riesgo por factores tales como edad, soledad o dependencia, sin que se requiera su interacción con las nuevas tecnologías. Para ello, se han digitalizado algunas de las funcionalidades analógicas del servicio municipal de teleasistencia que presta la Concejalía de Servicios Sociales del Ayuntamiento de Santander a través de un empresa externa, Atencia.

A través de una plataforma IoT y un conjunto de sensores domésticos desplegados en los domicilios de los usuarios finales, es posible monitorizar de forma remota la actividad de los usuarios finales en sus hogares y detectar situaciones de emergencia en base a un conjunto de reglas y alertas previamente configuradas.

Ilustración del piloto2

En este piloto participan dos tipos de usuarios:

- Los "usuarios finales" que son personas mayores que viven solas, son usuarios del servicio municipal de teleasistencia, y en cuyos domicilios se han instalado una serie de sensores tales como el sensor de ocupación de cama, el sensor de apertura de puerta/ventana, sensor de movimiento y un enchufe inteligente; y
- Los "usuarios" que son los teleoperadores de teleasistencia, que se encargan entre otras tareas de visualizar los datos de la actividad en el hogar de las personas mayores a través de un cuadro de mando y contactar con ellos ante posibles situaciones de emergencia.

A través de la concejalía de Servicios Sociales y la empresa Atencia, se realizó la selección de usuarios para participar en esta experiencia piloto, que lleva en funcionamiento desde septiembre del año pasado.

En este enlace podéis acceder al vídeo del piloto2.

M Sec Use Case 2 - Home monitoring security system for ageing people (Spanish subtitles)

Figure 2—23: Pilot2 information at Santander municipal website and video with Spanish subtitles

Data management

Table 2-8: Use Case2 data management

Type of data	<ul style="list-style-type: none">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	<ul style="list-style-type: none">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	<ul style="list-style-type: none">Over the course of the pilot, data is generated from sensors, and is collected and forwarded via MQTT by a Gateway Hub device in JSON format.MQTT channels were created upon the different measurements collected by the home sensors.The Tele-assistance back-end was subscribed to all these MQTT channels for each user to receive all the data from every home.
Data storage	<ul style="list-style-type: none">Over the course of the pilot, data are collected and entered into NoSQL database (MongoDB) as JSON documents.





Data protection policies and processes

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 an individual to make choices and to control how and with whom they share data collected by sensors), during the year 2 of the project, the consortium conducted an evaluation of the need to conduct a Data Privacy Impact Assessment (DPIA) as defined by the GDPR. The consortium based the criteria evaluation of the need of DPIA under GDPR (General Data Protection Regulation), Article 35 that sets out three types of processing and always requires conducting a DPIA⁴. Furthermore, the Treatment list of DPIA⁵ was analysed with eleven (11) criteria to be considered. During the assessment, any criteria were considered as applicable to the current use case.

The pilot has been tested within a small group of individuals, in total 5 end users. These users are above 65 years old but in any case, they are independent ageing people. For each of the participants, an informed consent has been signed (it can be found in D5.11 "M-Sec GDPR compliance assessment" submitted in M24), showing the purposes of the research, the procedures, potential inconvenience or benefits as well as the handling of their data (protection, storage).

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 have been collected. Minimization controls have been applied only to process personal data that are considered essential for conducting the pilot. Therefore, the consortium only collects data that are 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 has been adopted.

In addition, an agreement that regulates the processing of personal data and its respective responsibilities (ART.26 GDPR) has been signed between Santander Municipality (as the one in charge of tele-assistance service) and Worldline (as the one in charge of providing the solution) during year three, both are acting as co-controllers. The tele-assistance company, Atenzia acts as data processor and currently has a contract signed with Santander Municipality.

All the data gathered through questionnaires, interviews and focus groups have been anonymised for the purposes.

Below we present a fact sheet on which type of data has been processed.

Table 2-9: Fact sheet for Use-case 2

Data in encrypted database	All Personal data from users: name, initials of last name, mail (optional), address, phone number. Additionally raw data generated by the sensors.
-----------------------------------	--

⁴ <https://gdpr.eu/article-35-impact-assessment/>

⁵ <https://www.aepd.es/sites/default/files/2019-09/listas-dpia-en-35-4.pdf>





Data in blockchain	The hash of all the activity generated by a single user during one day. Why? To verify that a dataset has not changed. If the string generated differs from the previous one, then data has been modified.				
Does it involve personal data processing?	Yes	Please, specify which kind of data	Name, address, email, phone number of end users and name, email and phone number of caregivers (optional). Data related with home activity of the user (door/window open sensor, motion sensor, electricity consumed by a specific device).		
Data processing	<p>The main purpose of collecting data is to test a digital solution of telecare that includes multiple secure mechanisms developed within the context of M-Sec.</p> <p>1. Identification data:</p> <p>-Details: Name, last name, email (optional), phone number, address.</p> <p>-Justification: Necessary for creating the profile and communicate in case of an alert triggered.</p> <p>-Minimization controls: Name and last name is pseudoanonymized, address and phone number is not necessary as the ID of the user is used to be linked with the address and phone number storage in other systems from the tele-assistance company.</p> <p>2.- Living habits:</p> <p>- Details: Raw data from sensors.</p> <p>- Justification: Necessary to monitor the user.</p> <p>- Minimization controls: no.</p> <p>3. Status information:</p> <p>- Details: Text/messages from teleoperators related to users (i.e. tried to contact the user with no success).</p> <p>- Justification: For communication with other teleoperators that covers different schedules.</p> <p>- Minimization controls: No.</p> <p>4. Connection Data:</p> <p>- Details: Events logs (technical logs).</p> <p>-Justification: Required for maintenance purposes.</p> <p>- Minimization controls: No.</p>				
Data retention	One month after the finalization of pilot				
In case, there is personal data, please add the following details:					
DPO	AYTOSAN (protecciondedatos@santander.es) / WLI (maria-isabel.menamayor@worldline.com)	Controller	AYTOSAN/WLI	Processor	Third Party Tele-assistance





The screenshot shows the 'Senior Care' application interface. On the left is a sidebar with navigation links: Dashboard, Users, Devices, Rules, Platform Users, Global Statistics, and Teams. The main content area is titled 'Users - Maria Rodriguez'. Below the title are tabs for RULES, DEVICES, ACTIVITY, and CONTACT DETAILS. The 'DEVICES' tab is active, displaying a table of devices associated with the user. An 'EXPORT' button is highlighted with a red box in the top right corner of the main content area.

Alert	Device ID	Type of device	Location	Connectivity	Battery
	0300000100011AA8	Gateway	---		
	0301000100011AA8	Smoke sensor	Kitchen 5		
	0302000100011AA8	Mattress sensor	Bedroom main 5		
	0303000100011AA8	Door sensor	Main door 5		
	0304000100011AA8	Smart plug	Computer 5		
	0305000100011AA8	Smart plug	TV 5		
	0306000100011AA8	Motion sensor	Hall 5		

Figure 2—24: Senior Care Exports User's Data

The screenshot shows the 'Senior Care' application interface with the 'CONTACT DETAILS' tab selected for Maria Rodriguez. The user's profile information is displayed, including name, date of birth, address, email, and phone numbers. Below the profile information is a section for 'Caregiver' with details for Amparo García. At the bottom, a 'GDPR Data Delete' section is highlighted with a red box, containing a warning message and a 'Delete user' button.

GDPR Data Delete
If you proceed to delete the information, all personal data, assigned devices and the established rules over these will be erased. This action is irreversible.

Delete user

Figure 2—25: Senior Care Deletes User Action





Technical approach – M-Sec components

The pilot consists of the integration of several components from M-Sec as it can be seen in the figure below:

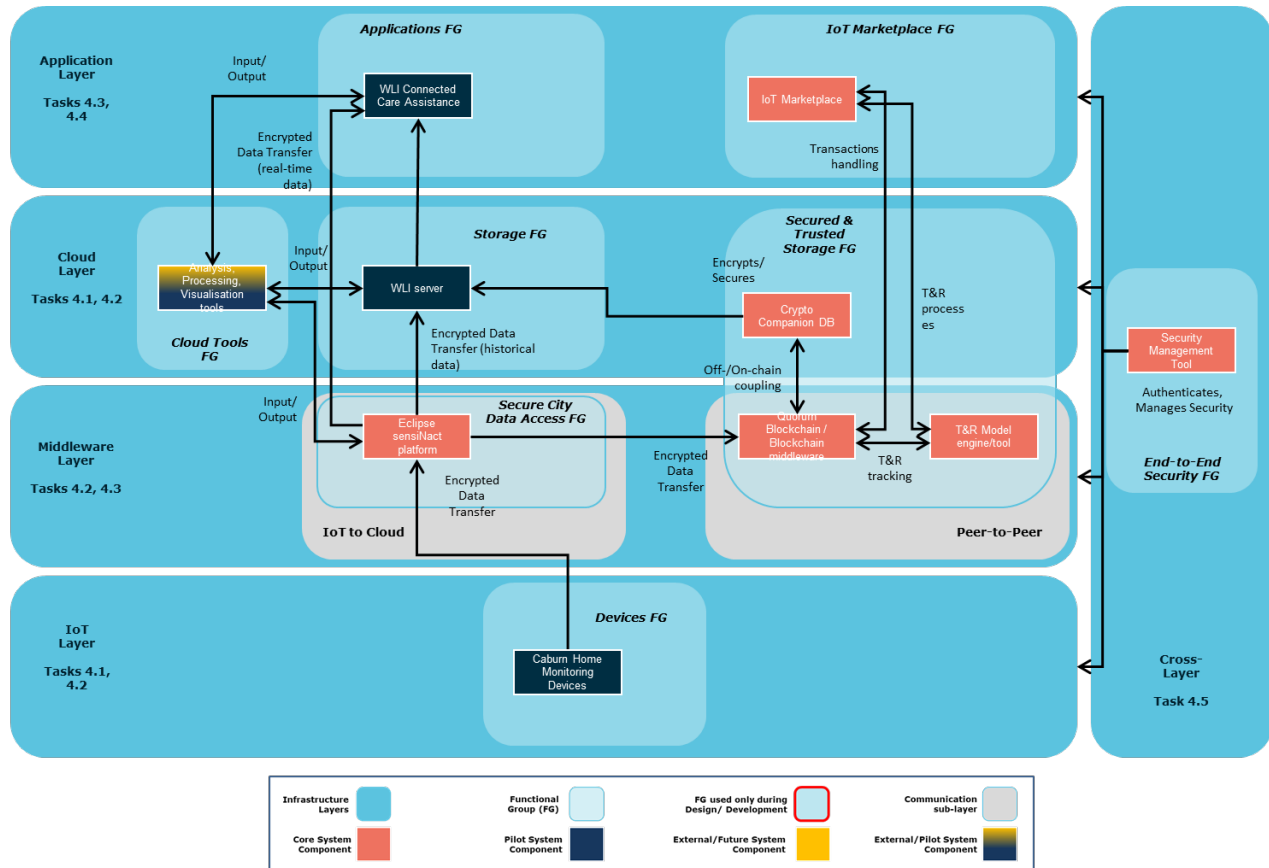


Figure 2—26: Senior Care and M-Sec interaction Diagram

On the IoT Layer, the solution is composed of a series of IoT Home sensors supplied by Caburn. Among them:

- **Squid.link Gateway:** The Squid.link Gateway is a modular platform for flexible Home Area Network. It connects wireless devices through a communication protocol and reports data back to the user's computer or smartphone. The Squid.link Gateway is configurable and an extremely flexible solution for connecting networks based on different technologies.



Figure 2—27: Squid Link Gateway Caburn

- **Door/Window Opening Sensor:** The Door/Window Sensor detects and reports the opening and closing of doors and windows. Easily installed on any door or window, the sensors trigger a signal when parted,





notifying the user when a room is entered. The Window Sensor also features a built-in temperature measuring functionality that measures changes in room temperature, down to a 0.1°C interval. Readings from the sensor can be sent via a home automation system through SMS, e-mail, or web. The increased awareness of temperature and daily power consumption can help your customer decrease their heating costs.



Figure 2—28: Door/Window Opening Sensor Caburn

- **Motion Sensor Mini:** The wireless Motion Sensor Mini is a compact motion sensor. The product includes an occupancy sensor, a light sensor, an alarm sensor, a temperature sensor, and a tamper switch. The provided mounting screws can be used to mount the Motion Sensor Mini in the corner or flat on the wall or ceiling. Alternatively, the included stand can be used to place the Motion Sensor Mini on a table or shelf.



Figure 2—29: Motion Sensor Mini Caburn

- **Smart Plug Mini:** The Smart Plug Mini is an intelligent, remotely-controlled adapter that monitors the power consumption and enables the user to control electrical equipment by switching it on or off remotely via ZigBee. The Smart Plug Mini is easy to use since it requires no installation. The user just has to put it into an electrical outlet and then plug in the desired electrical device.



Figure 2—30: Smart Plug Mini Caburn

- **Bed Occupancy sensor:** It is a pressure pad for a bed that monitors occupancy and automatically raises an alarm call if an unexpected activity is detected. It can identify if an individual has not gone to bed by a





specified time or if they have left their bed during the night and have not returned within unexpected time period.

All the data collected by the IoT home sensors are sent through MQTT to the Eclipse sensINact Platform. Eclipse sensINact is composed of two tools, sensINact Gateway aiming at integrating devices and aggregating data from various sources and sensINact Studio aiming at interacting with the sensINact Gateway to visualize the devices and the data. Thanks to its modular approach, avoids burden and complexity of system maintenance and evolution and allows replacing, updating, modifying software components in a seamless and dynamic way. In addition, it provides a fine-grained security mechanism to allow access to services by only authenticated and authorised entities.

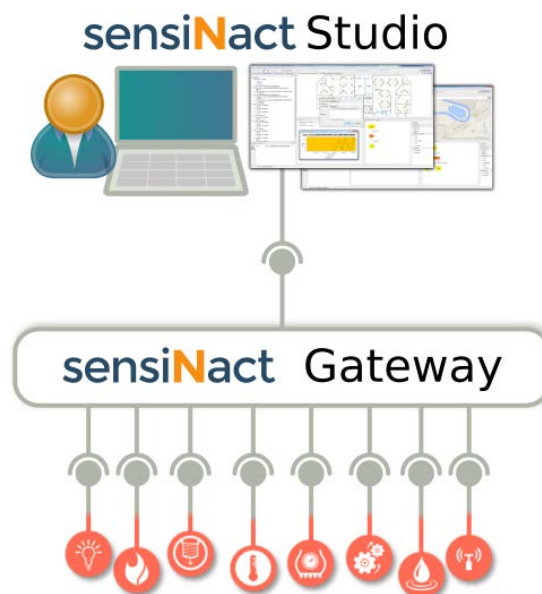


Figure 2—31: Eclipse sensINact Platform

Once data are collected, they are sent to the server, proceeding to encrypt sensitive data using the Crypto Companion Database (CCDB). The CCDB is a system that encrypts the data with an asymmetric public/private key pair. The data can only be accessed by the owner, who has to be authenticated, and the authorised operators allowed by the owner. At the same time, a hash is generated from all the encrypted data and stored in the Quorum blockchain for data tamper-proof.

Thanks to the Crypto Companion Database, rights to users can be provided to get all their information, delete all the information related to them and modify any detail.

The Use Case 2 uses an asset called Security & Storage Functional Group API that gathers all endpoints from the Crypto Companion Database and the blockchain. This API is secured by the Security Manager, providing a layer of authentication, so before using any endpoint a set of credentials has to be provided to the user of the API.

Data generated by all sensors of the use case are sent to the Marketplace, in order to keep privacy and any possibility of tracking a specific user, the data is anonymized. The process of anonymizing data consists of deleting any real identifier and any sensitive data from the users and their sensors. Those data that can be publically available because they do not contain any personal data related to the end user, are transferred to the M-Sec marketplace where stakeholders who may be interested in getting home activity data can buy the





data using M-Sec Tokens, which is a cryptocurrency in the form of a smart contract running in on blockchain. The deployed smart contracts communicate with each other to verify the sufficient funds of the buyer and complete the purchase by transferring funds from the balance of the buyer to one of the data owner.

The data generated in the use case are saved in a backup file every day in order to be able to recover missing data from outages or attacks.

Finally, at the application layer, Senior Care is the web application available for the tele-assistance party where to visualize all data and activity from end users, configure devices and alarms and manage users.

Pilot setup

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

Table 2-10: Use Case2 set up

Planning	<ul style="list-style-type: none">• Start Date: M26 (September 2020)• Duration: M26 – M39 (15 months)• Phases:<ul style="list-style-type: none">○ PHASE 1 – User Panel set-up (M19-M25): 5 end users selection & training. User consent.○ PHASE 2 – MVP release (M25): Sensors installation & calibration. Connectivity tests. Front-end applications tests. Proof-of-Concept oriented.○ PHASE 3 – 1st Trial of the pilot (M26-M38): Integration with the M-Sec platform. Iterative sub-releases.○ PHASE 4 – 2nd Trial of the pilot (M39): Iterative sub-releases.○ PHASE 5 – Pilot Evaluation (M39): Questionnaires. KPIs follow-up report.
Home set-up	<ul style="list-style-type: none">• Elderly homes have been set-up with different sensors and gateways connected to the M-Sec platform (Gateway, door/window sensor, smart plug, bed occupancy sensor, motion sensor).• All participating users have been informed of the pilot goals, duration and activities and their consent required.• Every participant has been provided with a sensor pack. They all contain a gateway hub for sensor connectivity.• The Tele-assistance company and care giving network has been provided with a web front-end displaying enriched monitoring & emergency data from users.

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 the design, validation and testing of the M-Sec framework in terms of security provided.

Table 2-11: Use Case2 KPIs





#KPI	Goal	How to measure?	Target	How to measure?
#Participants	Minimum number of end users to test the solution provided.	Number of end users (ageing people) registered into the system	≥5 users	Senior Care
#Daily Home Activity Data	To evaluate the volume of data generated and its scalability.	Raw data sent from the Home IoT sensors to Senior Care	<1GB	Senior Care
#Data frequency	To evaluate speed at which new data is generated	Latency time	≤25s	Senior Care
#Events that have occurred during the length of the pilot	In order to have a minimum sample where to verify reliability	Statistics Module	>100	Senior Care
#Events that have been handled during the length of the pilot	To evaluate the reliability of the alarms raised	Statistics Module	≥ 60 (4 alarms/month per user)	Senior 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.	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 Senior 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 (1 st Pilot Phase) >20 (2 nd 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	Senior Care
#End points accessed	Higher number of end points higher vulnerability grade	Access log file	<10	Whole System Pilot





Questionnaires

Two types of questionnaires in paper format have been provided in order to collect feedback and improvement areas during the pilot trial. One for teleoperators from Atenzia in charge of monitoring ageing users and the second one to end users (older adults). Results from these surveys can be found in D2.8 M-Sec validation and overall evaluation.

Atenzia Questionnaire

1. What is your role at Atenzia?
.....
2. What is your gender
Male ☐ Female ☐
3. How easy was Senior Care to use? *(From a scale from 1 (very unsatisfied) to 5 Very satisfied)*
1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐
4. How would you score the look&feel of the solution provided? *(From a scale from 1 (very unsatisfied) to 5 Very satisfied)*
1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐
5. Did Senior Care help solve your problem/achieve your goal? *(From a scale from 1 (very unsatisfied) to 5 Very satisfied)*
1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐
6. How easy was the installation procedure of the home sensors at the user's home? *(From a scale from 1 (very unsatisfied) to 5 Very satisfied)*
1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐
7. To what extent do you feel safer using the Senior Care system? (feeling of safety/reliability, acceptance) *(From a scale from 1 (very unsatisfied) to 5 Very satisfied)*
1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐
8. How well does the Senior Care system complement the existing analogic system to monitor ageing people? *(From a scale from 1 (very unsatisfied) to 5 Very satisfied)*
1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐
9. How easy is it to detect a non-regular behavior of a user through the alerts system implemented? *(From a scale from 1 (very unsatisfied) to 5 Very satisfied)*
1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐
10. How reliable do you think the information is provided by the Senior Care system is? *(From a scale from 1 (very unsatisfied) to 5 Very satisfied)*
1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐
11. How interested would you be in using Senior Care after the end of the test period? *(From a scale from 1 (very unsatisfied) to 5 Very satisfied)*
1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐
12. According to your personal view, to what extent do you believe that Senior Care and the M-Sec Project can help to reduce the breach about current security concerns in terms of data protection and increase user trust? *(From a scale from 1 (very unsatisfied) to 5 Very satisfied)*
1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐





13. How concerned would you be about your privacy when using Senior Care? *(From a scale from 1 (very unsatisfied to 5 Very satisfied)*

Very concerned ☐ Moderately ☐ Slightly ☐ Not at all ☐

14. Compared to the current analogic system used by Atenzia, how would you evaluate the accuracy of Senior Care? *(From a scale from 1 (very unsatisfied to 5 Very satisfied)*

1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐

15. Were there any false detections?

Yes/No

Please, specify details if yes.

16. Did you collect any feedback or impressions from the end-users who provided the tip about the following aspects:

a. Do you think that users perceived the security and trustiness on the system?

Yes/No

Please, specify details if yes.

b. Do you think that users found the procedure to test the solution well-explained?

Yes/No

Please, specify details if yes.

c. What do you think are the main drivers for users to participate in the tele assistance service offered by Atenzia?

Yes/No

Please, specify details if yes.

d. Do you think that users will speak about it with friends and relatives about this particular pilot testing Senior Care?

Yes/No

Please, specify details if yes.

17. Lessons Learned:

a. What worked well



Please, specify details if yes.

b. What didn't work so well?

Please, specify details if yes.

c. What is still needed to make the solution more interesting for Atenzia? (e.g. new functionalities?)

Please, specify details if yes.

18. How would you assess the collaboration with Worldline as the technical partner provider of Senior Care? *(From a scale from 1 (very unsatisfied) to 5 Very satisfied)*

1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐

19. Please, rate your overall satisfaction with the solution itself, the technical support and the M-Sec contribution in terms of security. *(From a scale from 1 (very unsatisfied) to 5 Very satisfied)*

1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐

20. Comment Box (Here you can provide any additional feedback or clarifications you may have on the answers).

.....

End-Users Questionnaire

1. Did you feel safer with the sensors installed in your home?
Yes ☐ No ☐
2. Have you ever felt your intimacy invaded?
Yes ☐ No ☐
3. Have the installed sensors caused you any inconvenience at any time?
Yes ☐ No ☐
4. Do you think that any other type of sensor would be helpful?
Yes ☐ No ☐
5. Would you recommend this pilot to family and friends?
Yes ☐ No ☐





Summary – lessons learned, sustainability

Regarding lessons learnt, two aspects did not work as expected:

- Bed occupancy sensors were not working properly. The main problem was the connection between bed mattress and sensor. It has been addressed with the supplier of the devices.
- The integrated prototype with M-Sec components. After performing all integrations with sensiNact, Security Manager, Marketplace, and the Blockchain Middleware and testing them on a development environment, the standard procedure to promote the software to a production environment was performed. Once the software was on production we faced some problems and new challenges. One of the problems was to overcome the downtimes in the Blockchain Middleware and the Marketplace, due to the huge fires in Greece, by creating some new software, as quick as possible, called “bridges” in order to let the system work properly even without communication. These new “bridges” were a challenging task because of the importance and the time we had. Another problem was due to the stress testing performed in the Security Manager system that made the servers unstable some days and let us with a communication problem. The Crypto Companion DataBase is secured by the Security Manager, and could not be accessed in a proper and stable way to save and retrieve data. After analysing this situation we could not find a proper way to solve this downtime, as the security was entirely delegated to the Security Manager.

In addition, even though an export method was implemented to analyse data collected from sensors, Atenzia required to have a new feature to export the data in an aggregated way from all users registered in the platform. This will help in the preparation of a report to be submitted to the municipal Social Services service on the results of the pilot.

Overall, Atenzia staff who have participated during the Senior Care pilot phase trial feel quite satisfied with the ease of use of the tool and the look & feel of the solution provided. They also highlight the ease of detecting unusual behaviours of end users through the alert system implemented. One of the key aspects is that thanks to M-Sec, it has been possible to bridge the gap on current security concerns in terms of data protection and increase user confidence. Finally, in terms of home sensors, they highlighted the ease of their installation.

With regard to end users, those who have had several home sensors installed in their homes, in terms of security, all participants reported feeling safer with the new sensors installed in their home. In terms of privacy, all agreed that none of them had their privacy invaded at any time.





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

Pilot scenario and objectives

UC3 is a pilot that builds a secure IoT platform for smart cities by integrating the multi-layer security assets of M-Sec partners based on the Keio mobile sensing platform that has been conducting demonstration experiments with Fujisawa City for more than 3 years.

In that sense, UC3 originally used the above-mentioned garbage truck sensing as a use case, but it is the secure IoT platform itself for smart cities, which is the purpose of the M-Sec project.

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 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.



Figure 2—32: Mobile Sensing by 60 Garbage trucks in Fujisawa city

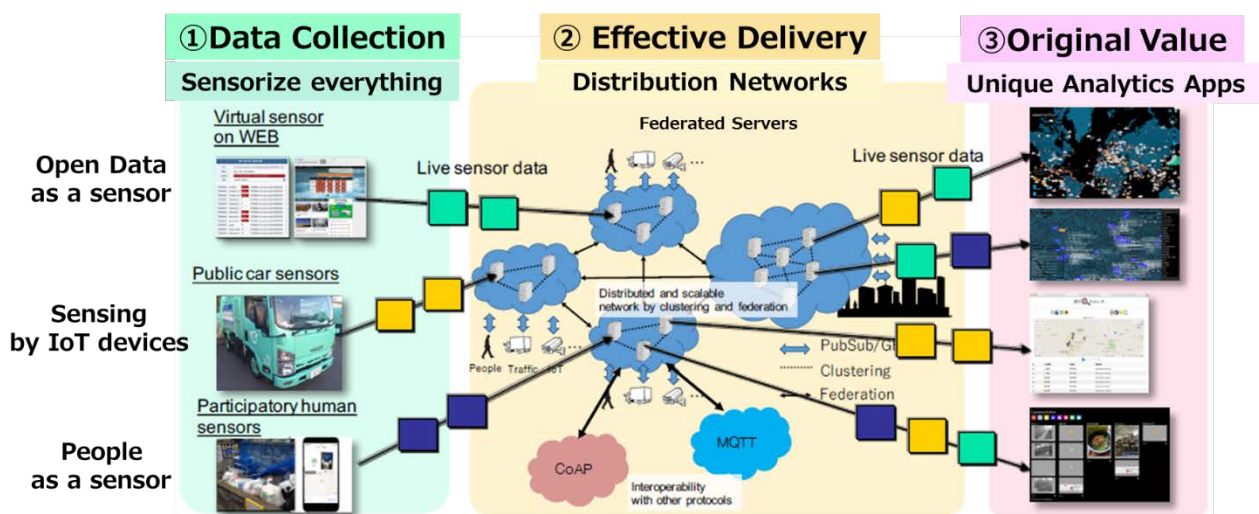


Figure 2—33: Keio mobile sensing platform based on SOXFire as IoT platform for Smart city



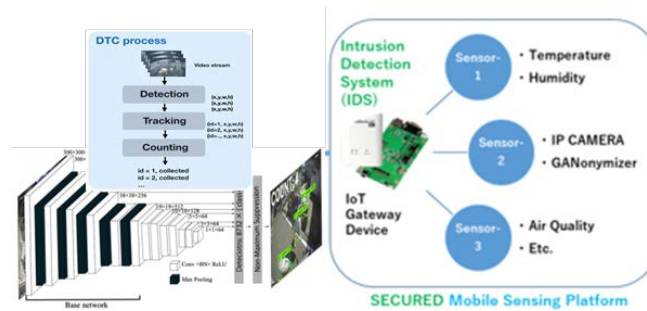


Figure 2—34: M-Sec Secure solutions which is integrated in Keio mobile sensing platform

Challenges and mitigation actions on pandemic situation

UC3 has focused on verifying a secure mobile sensing platform using garbage truck sensing as an application example. If you think of it as one IoT application, like other UCs, the pandemic environment of COVID-19 has an impact on the experiment. For example, the participation of stakeholders, such as Fujisawa City and cleaning companies, which are essential for garbage truck sensing experiments, was restricted. Therefore, as shown in Table 2-12, the scale of the experiments in the actual field was reduced, and we conducted the experiments and verifications at the laboratory level in order to cover this pandemic situation.

In addition, since UC3 is a UC that focuses on the verification of the secure mobile sensing platform, verification was carried out by several applications in addition to the initial cleaning vehicle sensing. For example, in order to solve the requirements of the pandemic environment as a countermeasure against COVID-19 infection, the ventilation status of restaurants in Fujisawa City was constantly monitored, and these data were input to the secure mobile sensing platform. In addition, we demonstrated that data such as the ventilation status inside the route bus, which is public transportation, and the ventilation status in the classroom on the university campus were used as inputs for the secure mobile sensing platform. We have achieved stable secure mobile sensing platform by completing all of these experiments..

Table 2-12: Use Case3 Challenges & Mitigation actions

Challenge	Description	Mitigation Action
1	The mounting plan is delayed due to the COVID-19 pandemic and the available time for experiment will decrease.	Ensure that the UC can be tested at the minimum scale.
2	The time to troubleshoot or improve results has also reduced due to the COVID-19 pandemic and available time for experiment.	Ensure that the UC can be tested for at least one month for 1 st stage, then make improvements and re-test for a minimum of one month to meet the deliverable deadlines.





Engagement process with citizens and stakeholders

Unlike other UCs, UC3's Secure Mobile Sensing Platform is positioned to realize a secure and globally expandable smart city platform. Therefore, for example, it is positioned to provide a foundation for realizing UC4 and UC5. Therefore, unlike other UCs, citizens and communities are not direct users, but are indirectly involved with citizens and communities through UC4 and UC5 applications.

For example, in a "Garbage Truck Sensing" that has been ongoing with Fujisawa City for more than three years, we have installed sensor boxes on 60 garbage trucks in collaboration with the community of garbage collector companies in Fujisawa City. In addition, we installed an Edge Device on the garbage trucks to implement a "Deep Counter" that automatically analyses the amount of garbage collected using deep learning, and only the analysis results are displayed without uploading images that pose a privacy issue to the cloud. These are achieved through close collaboration with Fujisawa City and the community of garbage collector companies.

There is no direct end user for UC3, but Pilot dissemination for replication purposes has been done in parallel since the initiation of the pilot in August 2020. Some of the actions conducted are:

- Use Case Blogpost where use case description is showed, including challenge it addresses, the M-Sec specific approach, the pilot implementation and results as well as the value proposition and the business model canvas. Available [here](#).
- UC Brochure where the unique value proposition is detailed as well as the main stakeholders interested on such a solution, features provided and pilot testimonies. Available [here](#).
- UC Video as a demonstration of the solution and the M-Sec value added. Available [here](#).



Figure 2—35: Pilot3 Blogpost and Brochure



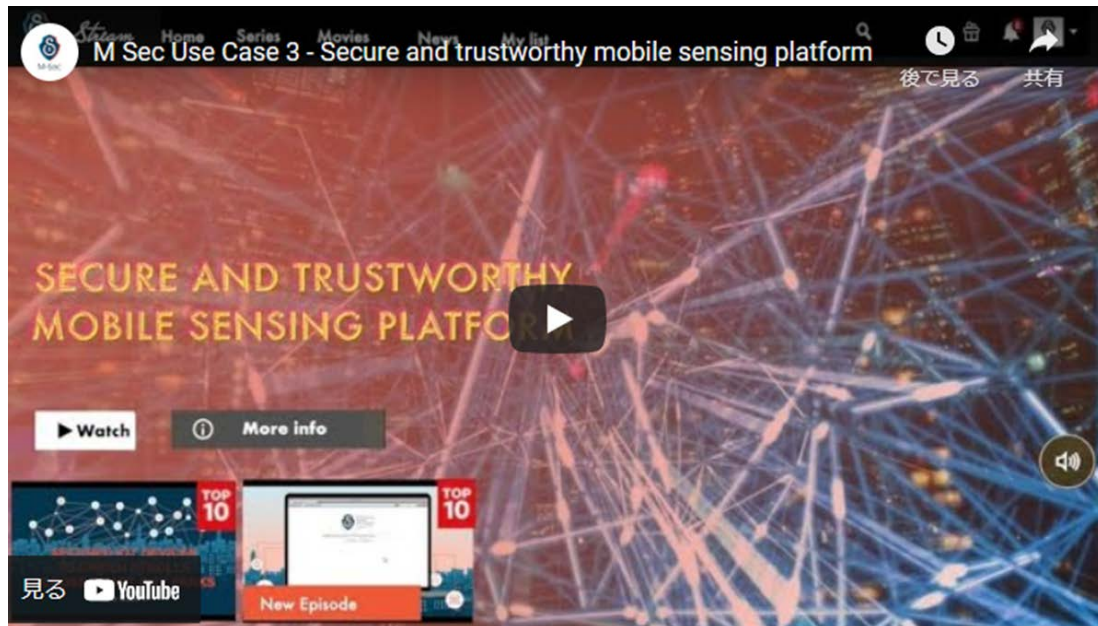


Figure 2—36: Pilot3 Videos in English; Japanese & Spanish

Data management

Table 2-13: Use Case3 Pilot 3 data management

Type of data	<ul style="list-style-type: none">• Raw data values from garbage truck sensors (temperature, humidity, atmospheric pressure, illuminance, UV-A, PM2.5, acceleration, angular velocity, compass, position, camera, etc.)• Smartphone application data from “SmileCityReport” (photo, comment, smile, GANonymizer on/off, time, user, theme, points, etc.)• Raw data values from Restaurant environment sensing sensors (CO2, PM2.5, temperature, humidity)• Raw data values from Class room environment sensing sensors (CO2, PM2.5, temperature, humidity)• Raw data values from Public Bus environment sensing sensors (CO2, PM2.5, temperature, humidity)• Smartphone application data from “MinaRepo” (photo, comment, time, reporter, theme, etc.)• Web scraping data from “Sensorizer” (Weather, River water level, precipitation amount, Traffic jam, etc.)• Metadata associated with raw data (network link strength, AC frequency, sensor type, data unit type, transaction type, etc.)• Transducer data associated to each SOXFire data
Format of data	<ul style="list-style-type: none">• SOXFire data that implements the Sensor-Over-XMPP (SOX) format in the Openfire payload and manages sensor information• JSON data exchange format for transporting data & metadata within an MQTT channel.• Metadata will be generated to describe the data generated sensors in each sensing.
Data collection	<ul style="list-style-type: none">• The data supply side in each sensing publishes the data to SOXFire, the data is collected via Keio Secure SOXFire, and the data receiving side subscribes to optimally distribute all the data.





Data storage

- The data collected by each sensing is stored in the database of Keio Mobile Sensing Platform and the linked system.

Data protection policies and processes

The Secure and trustworthy mobile sensing platform use-case is about collecting environmental data using instrumented garbage trucks. Those trucks are equipped with sensors such as temperature, humidity and pollution but are also equipped with a camera in order to extract information from video streams. This analysis is made on-board and only computed values are forwarded to the system using SOXFire.

Table 2-14: Fact sheet for Use-case 3

Data in encrypted database	- temperature and humidity, PM2.5, acceleration sensor - analyzed data by analytics apps including deep learning on edge computing environment		
Data in blockchain	Anonymized environmental data		
Does it involve to process personal data?	No (this pilot is focusing on platform capabilities)	Please, specify which kind of data	N/A
Data Processing	1. Garbage collection activity data - Details: Counting data from sensors and video data - Justification: Necessary to monitor the collection activity - Minimization controls: no 2. Climate or geography information - Details: Raw data from sensors - Justification: measure the climate and geography condition - Minimization controls: No		
Data Retention	From the beginning of the 1 st pilot, to 10 years after the corresponding research output (e.g., a paper) is published.		

Measures to comply with Privacy strategy on APPI

APPI is not applied because personal information is not handled.

Technical approach – M-Sec components

The following figure shows the architecture of defined for Pilot 3.



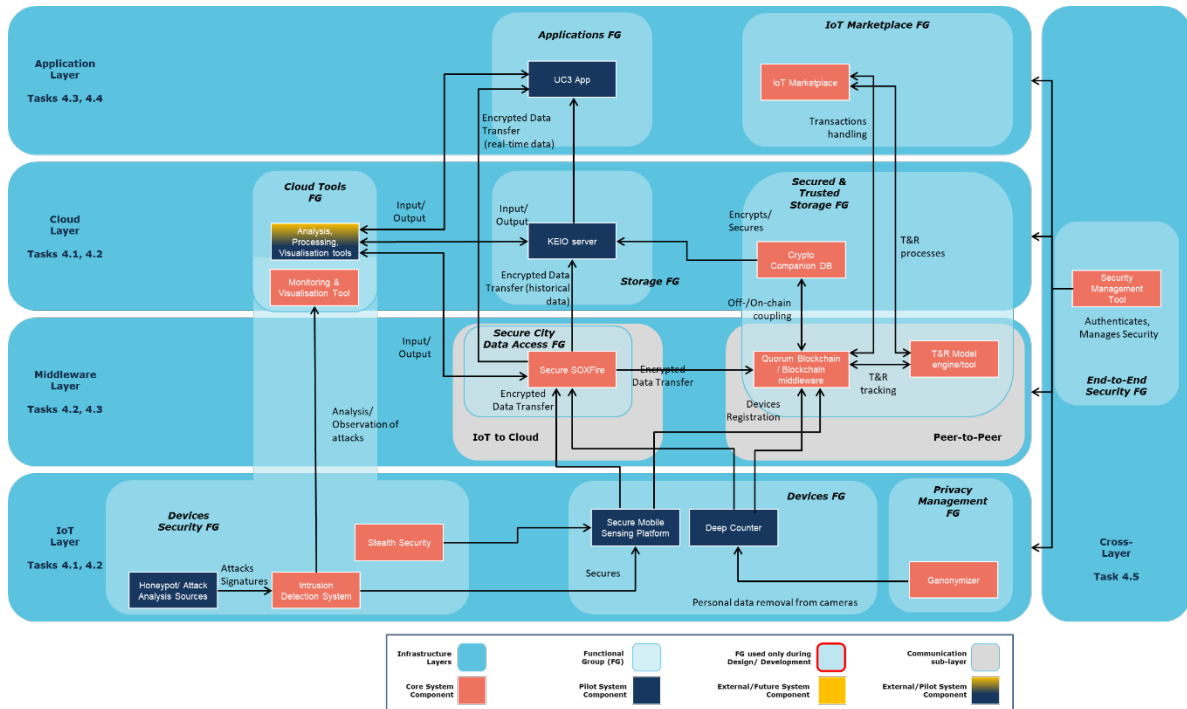


Figure 2—37: Architecture of Use Case 3

UC3's Secure Mobile Sensing Platform was realized by incorporating the security solutions of M-Sec project partners into the platform for smart cities centered on Keio SOXFire, which has already been proven in Fujisawa City. Multiple layers of security were provided through hardening, encryption, intrusion detection, intrusion prevention, stealth security, monitoring and visualization tools.

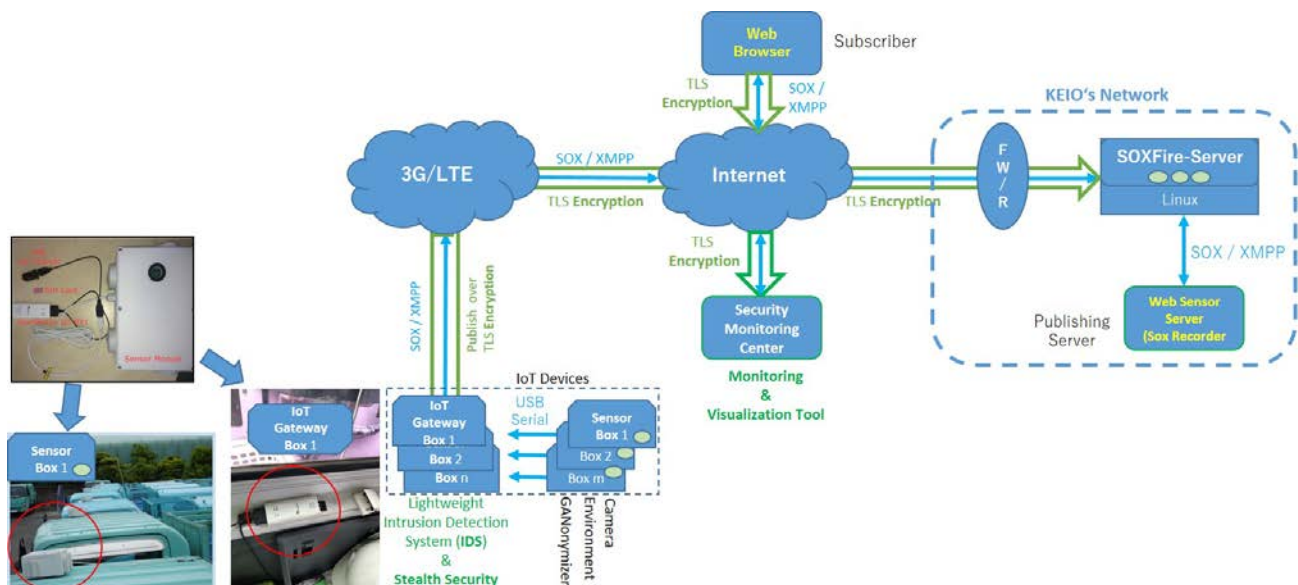


Figure 2—38: Use Case 3 detail





Pilot setup

Table 2-15: Use Case3 set up

Planning	<ul style="list-style-type: none"> • Start Date: M29 (December 2020) • Duration: M29 – M37 (9 months) • Stages: <ul style="list-style-type: none"> ○ Stage 1 – Pre-Final integration in order to test SOXFire and Security solutions. ○ Stage 2 – Final Testing in order to collect data for final evaluation.
Mobile Sensing Platform setup	<ul style="list-style-type: none"> • Build an environment to send data from the sensor boxes installed in 60 Garbage Trucks in Fujisawa City to the Mobile Sensing Platform. • Install an edge device in the Garbage Truck for "Deep Counter" that automatically detects the amount of dust discharged. • Build a Secure Mobile Sensing Platform based on the system that incorporates some security Solution from an M-Sec partners into Keio SOXFire.

KPIs

As with other UCs, the initial KPI achievement is in a little bit difficult situation in the situation of COVID-19. However, unlike other UCs, UC3 is the platform itself, so the current update from the perspective of platform users is as follows:

Table 2-16: Use Case3 Pilot3 KPIs

#KPI	Goal	Target	How to measure?
# platform users	Having multiple common platform users as a secure and trustworthiness mobile sensing platform.	3	10 (garbage truck sensing, SmileCityReport, Restaurant environment sensing, class room environment sensing, outside environment sensing, public Bus environment sensing, MinaRepo, Sight Seeing Area sensing, Amusement Park sensing, Sensorizer)
# Anonymization	Functional verification of privacy data protection	More than 20 privacy-related objects	56 GANonymizer from SmileCityReport
# Secure Data Processing	Securely distributes data as a Secure Trustworthiness mobile sensing platform.	More than 50 kinds of data	More than 50 (11 kinds of data from garbage truck sensing, 8 kinds of data from SmileCityReport, 4 kinds of data from Restaurant environment sensing, 4 kinds of data from class room





#KPI	Goal	Target	How to measure?
			environment sensing, 4 kinds of data from outside environment sensing, 4 kinds of data from public Bus environment sensing, 5 kinds of data from MinaRepo, 2 kinds of data from Sight Seeing Area sensing, 2 kinds of data from Amusement Park sensing, more than 10 kinds by Sensorizer (Weather, River water level, precipitation amount))
Scan attempts blocked	Hackers frequently scan the internet to find open ports or services available on a device before an attack. Blocking scan can help reduce the attack surface.	90% or more	Using the security monitoring tool
Ping/ICMP packets blocked	Hackers need to know the IP address of their target for which they commonly use Ping/ICMP packets. Blocking this can make it difficult for them to pinpoint an attack	90% or more	Using the security monitoring tool
Telnet access blocked	Telnet service is one of the highest exploited service for breaking into a device remotely. Blocking it would avoid such attacks.	90% or more	Using the security monitoring tool
SSH access blocked	SSH is another service that is commonly under attack to gain remote access to the controls.	90% or more	Using the security monitoring tool
Misc. attacks blocked	There are many kinds of attacks conducted by various bad actors that are flagged by the threat intelligence communities. IDS/IPS can summarize various attacks based on their signature to block them from succeeding. This will help the solution to block any such flagged attacks.	90% or more	Using the security monitoring tool

Questionnaires

Unlike other UCs, UC3 is regarding the mobile sensing platform itself only. So there are no end-user questionnaires.

Summary – lessons learned, sustainability

UC3 realizes a secure smart city platform by combining the sensing data from the sensor box installed in the garbage truck, which Keio University has been promoting in collaboration with Fujisawa City, with the security solution of the M-Sec partner. This is exactly one of the important activities of the M-Sec project as a whole,





in the sense that it enables the conflicting requirements both "security" and "open IoT platform" for smart cities that widely distributes IoT data.

Although UC3 pilot collects the city's environmental data and garbage emissions from garbage trucks as an example, this secure IoT platform can also manage various data collections such as the environmental data at restaurants in Fujisawa City, the environmental data in classrooms on university campuses, the environmental data at bus routes/public transportation, data on the Web, and the participatory sensing data from the smartphone app "SmileCityReport" like UC4.

In this way, UC3 Secure Mobile Sensing Platform has established the foundation of a secure IoT platform for flexible and scalable smart cities that can efficiently collect and distribute various city data.





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

Pilot scenario and objectives

UC4 explores the possibility of secure sharing on citizens' affective information and information on the city. In the city, there are many different events occurring every day. As a means of detecting/sensing such occurring, participatory sensing solutions that let people (citizens and possibly additional visitors) report such events, from their own (human's) perspective, with their mobile devices (e.g., smartphones), are getting popular. However, protection of privacy information in such sensing methodology was yet to be explored, thus it is the main focus of this use case. By using "SmileCityReport" (affective participatory sensing platform on mobile devices), "Ganonymizer" which enables edge-(mobile)-side computation for privacy protection, and SOXFire for secure data sharing of sensed information, the users' photo-based report on a local happening will be shared among multiple users, after privacy protection processing of the taken photos. Moreover, the photo reports are securely shared only among defined "groups" in SmileCityReport so that only the member user can view the photos each other. As a cross-border use case, this use case focuses firstly on Fujisawa and then, it was expanded to Santander, providing a cross boarder use case.

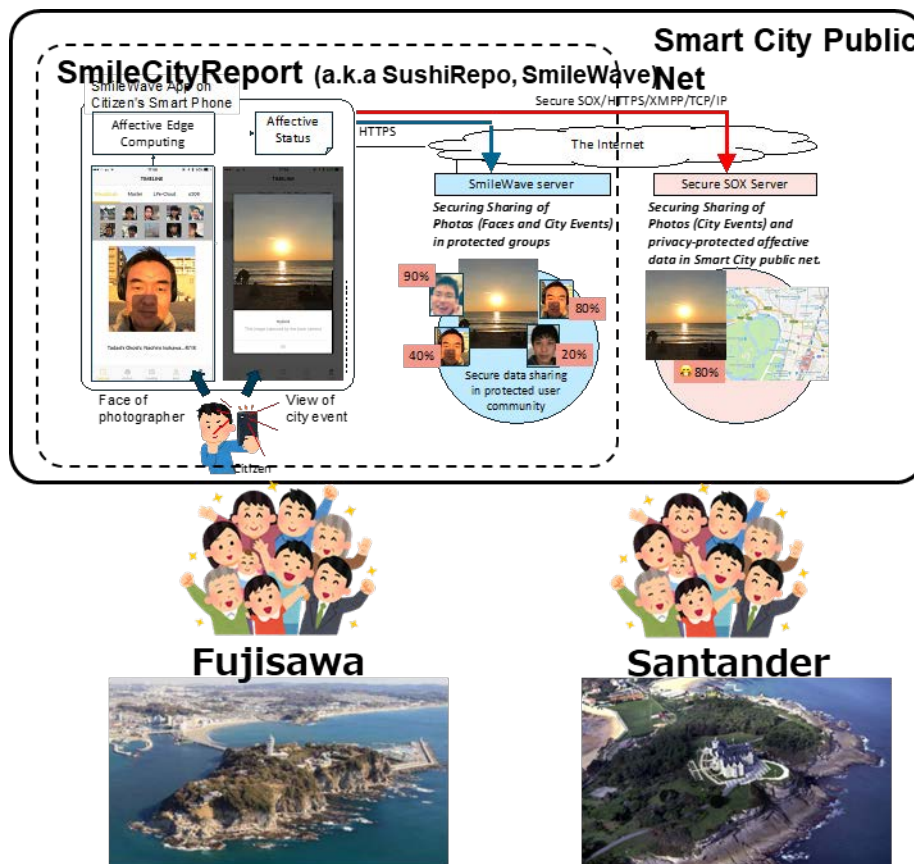


Figure 2—39: UC4 Overview





Challenges and mitigation actions on pandemic situation

Table 2-17: Use Case4 challenges and mitigations

Challenge	Description	Mitigation Action
1	The collaboration events were cancelled or postponed due to the COVID situation.	Setup a long-term field trial period instead of one-off.
2	Not to get in touch with event organizers(stakeholder)	Setup meetings periodically to come up with other ideas for field trials.
3	Low number of participants	Plan to set up Stamp Rally event for a long period of time. Prepare awards.
4	Technical issues related to i.e., mobile models or operating system required to run the SCR app may impact in the number of participants	Plan to register in the app store for and google play for users to install SCR instead of test tools such as Test Flight.

Engagement process with citizens and stakeholders

UC4 pilot is planned as following 3 PHASEs as described in section pilot setup:

- **PHASE 1 – Fujisawa City Event** (M28): The 1st UC4 actual pilot at “Fujisawa Jazz Meetin’ 2020” on 7th November 2020
- **PHASE 2 – Fujisawa City Pre-Final Trial** (M36 – M37): Pre-Final pilot in Fujisawa city by 260 user participants
- **PHASE 3 – Cross Border Trial with Santander** (M39): Final pilot as actual cross border pilot EU and Japan

We have setup default themes of SmileCityReport for each PHASE in order to collect user’s post as much as possible.

In the severe situation of the COVID-19, UC4 first conducted an actual demonstration at an event in Fujisawa City. Specifically, at the event "Fujisawa Jazz Meetin’ 2020" (<https://sfjm.info/>) in Fujisawa City held on November 7th in 2020, the first demonstration experiment was conducted using the 1st version of SmileCityReport.

The two venues set up in front of Fujisawa City Station were managed to maintain a social distance, and were held while restricting visitors and conducting health checks.





Figure 2—40: Fujisawa Jazz Meetin' Photos

We set up an M-Sec booth in a corner of the venue headquarters and planned a stamp rally using the UC4 smartphone app "SmileCityReport". At the booth, M-Sec members provided support for installing "SmartCity Report" on iPhone and Android.



M-Sec "SmileCityReport" Booth



Figure 2—41: M-Sec SmileCityReport Booth and Flyer

In the COVID-19 environment, almost everyone is wearing a mask, so it was not possible to demonstrate the function of reporting Smile by the photographer's image of the original SmileCityReport, but the following, according to the content of the event five themes, were set as default settings, and many reports were entered by participants.










Icon	Default Theme	Explanation
	What is the main venue like?	<p>Please give us a report on the main venue!</p> <p>Please tell us about the groups currently playing at the main venue and the excitement of the venue!</p> <p>If you don't mind, please include your smile image!</p>
	What does the street venue like?	<p>Please give us a report on the street venue!</p> <p>Please tell us about the groups currently playing at the street venue and the excitement of the venue!</p> <p>If you don't mind, please include your smile picture!</p>
	Anxious artist	<p>Please tell us the artists you care about!</p> <p>If you know, please tell us information about your favorite artists!</p> <p>If you don't mind, please include your smile picture!</p>
	Nice restaurant, recommended menu	<p>Please tell us a nice shop or recommended menu!</p> <p>If you don't mind, please give me your smile picture!</p>
	Congestion situation	<p>Please report the congestion situation!</p> <p>Please tell us about the congestion situation that everyone is interested in, such as enjoying Jazz with peace of mind!</p> <p>If you don't mind, please give me your smile picture!</p>

Figure 2—42: SmileCityReport Themes for Fujisawa Jazz Meetin'

In PHASE1, we have collected user's post as follows:

Table 2-18: Actual number of reports by user in PHASE 1

Theme	# of posts	# of comments	# of GANonymizer
	Fujisawa	Fujisawa	Fujisawa
Theme for testing	6	1	1
Congestion Status	23	1	5
Recommended Restaurant	7	4	2





Theme	# of posts	# of comments	# of GANonymizer
	Fujisawa	Fujisawa	Fujisawa
Anxious Artist	5	0	0
What does the street venue look like?	15	1	0
What does the main venue look like?	28	1	0
Total	88	8	8

PHASE 1 Participants: 16 (Fujisawa)

At UC4 Pilot PHASE1 held in Fujisawa City in November 2020, there were many posts about the venue situation and congestion situation as a citizen event held in the environment of COVID-19. In addition, because there were many event scenery posts, there were many photos including privacy objects of the general public citizens, and GANonymizer was particularly effective.

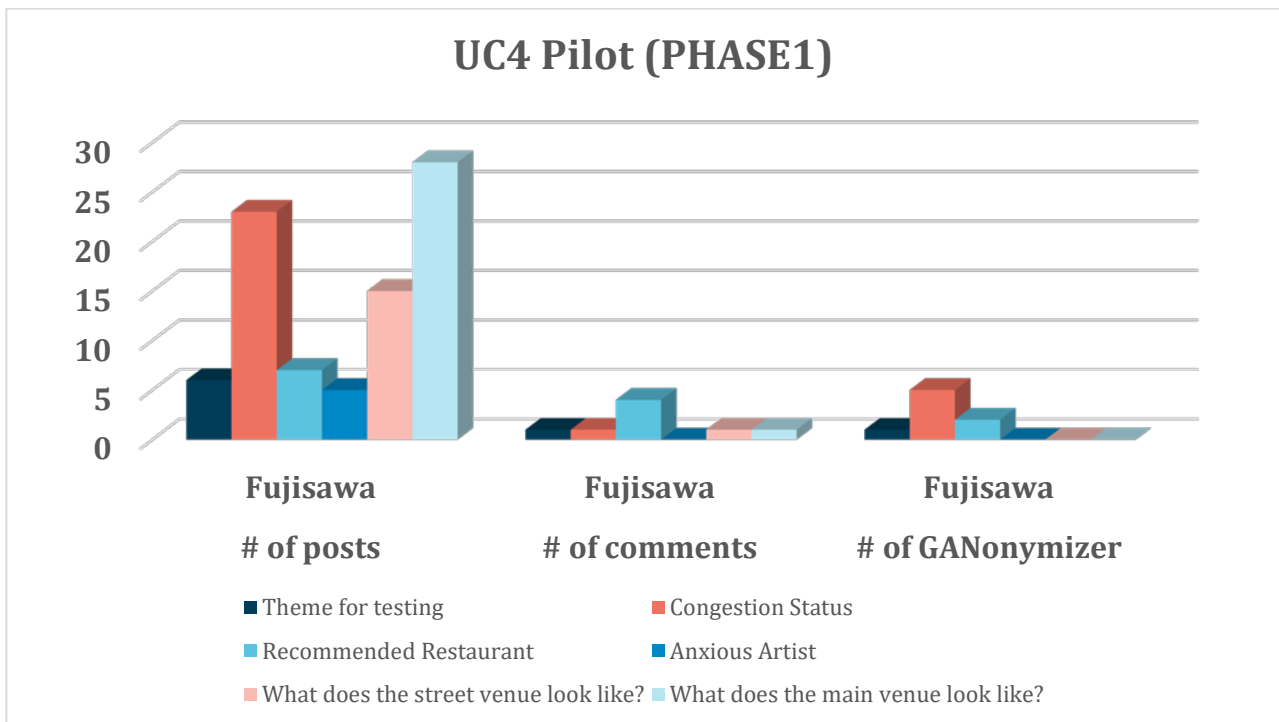


Figure 2—43: Results of UC4 Pilot (PHASE 1)

In PHASE 2, we applied following 4 default themes:






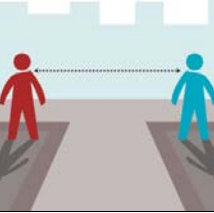


Icon	Default Theme	Explanation
	[Preserved version] Share with everyone · Superb view of this city	Show off our city with beaches, parks and gardens, sunset / night views, iconic buildings ... and your favorite spots! And your smile too.
	[What m?] Maximum social distance scenery	How far are you going !? Post a "extraordinary" social distance boast that can prevent corona infections. Welcome stories that make you laugh.
	[There was such a method!] My proud corona measures	There was such a method! Please show us your proud corona countermeasures that will make you unintentionally convinced and growl. Come with your smile as the creator.
	Takeaway gourmet pride	Let's brag about home-cooked food, delivery, and delivery gourmet! In addition to the impactful photos, your smile before eating.

Figure 2—44: SmileCityReport Themes for UC4 pilot PHASE2

In PHASE2, more than 250 users participated from Fujisawa city, and we collected the following user's posts for each theme:

Table 2-19: Actual number of reports by user in PHASE 2

Theme	# of posts	# of comments	# of GANonymizer
	Fujisawa	Fujisawa	Fujisawa
Beautiful spot of the City	996	878	16
Maximum Social Distance	218	33	2
My proud COVID-19 measure	65	32	11
Recommended gourmet	61	25	5
Total	1,340	968	34





PHASE 2 Participants: 250 (Fujisawa)

At the UC4 Pilot PHASE2 held in Fujisawa City in August 2021, despite the COVID-19 situation, 250 participants from Fujisawa City posted a total of 1,340 messages. There were comments from other participants received for more than 72% of the number of posts, so there were many interactions among citizen participants. On the other hand, unlike PHASE1, it was not a physical city event, but a post entirely from an individual, so the general public was rarely photographed, and there were few posts using GANonymizer.

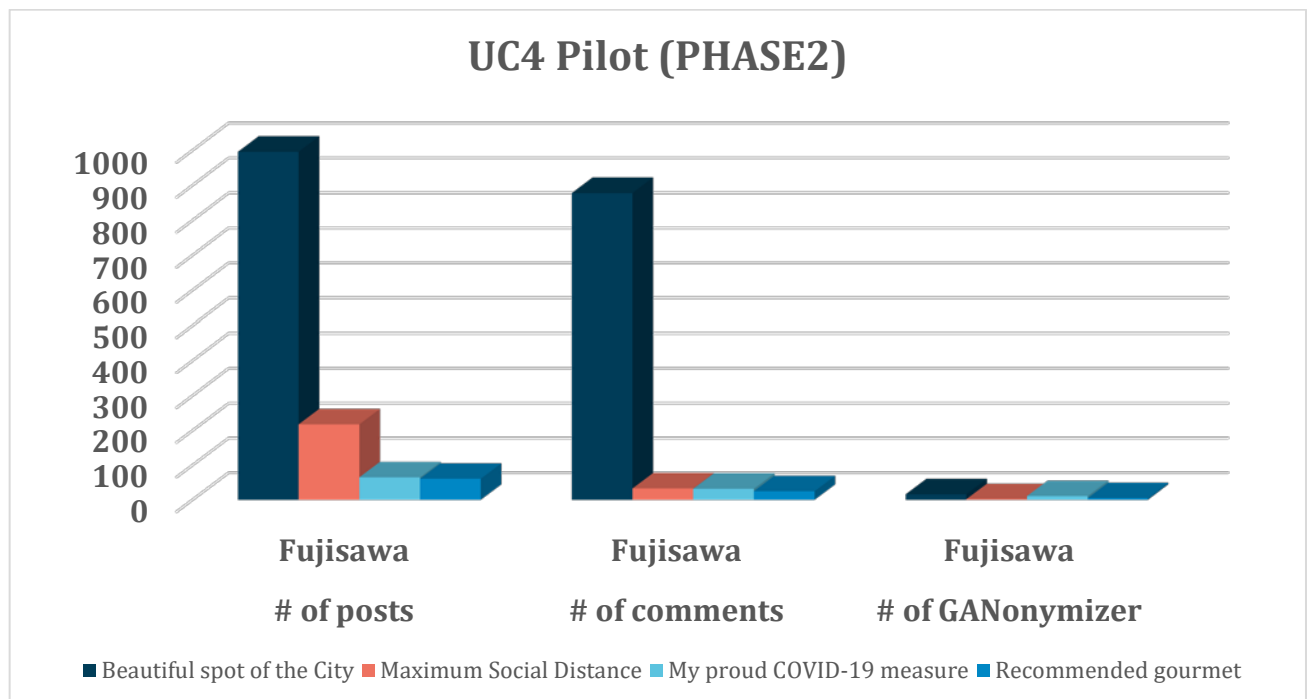


Figure 2—45: Results of UC4 Pilot (PHASE 2)





Figure 2—46: Users' post from each theme PHASE2

Cross-border extension

The launch of the cross-border pilot in the last month of the project is the result of close collaboration between the European and Japanese partners over many months. In this sense, and as mentioned in section 2.1, Santander City Council's strategy to involve citizens and stakeholders in this type of pilots includes two phases: a first phase with a small group of users, what we call friend-users, people who have participated in pilot experiences in other European projects and municipal staff from the departments involved in the pilot. Taking into account the feedback obtained in this first stage, it is decided to move on to the second stage, which includes the opening to a wider public, either a larger group of users or the whole population of the city. The robustness and stability of the solution to be validated will determine the openness of the pilot to a wider audience.

Before continuing with the involvement of the participants, it is important to note that this cross-border pilot has faced many different constraints from the very beginning:

- From a data protection point of view, the fact that an app developed in Japan is used in Europe has meant additional work, which is explained in the section on 'Data protection policies and processes'. This barrier has been overcome with the close collaboration between Keio University, developers of the SmileCityReport app, Santander City Council, through its DPO, and CEA & NTTDMC as privacy officers of the M-Sec project.
- From a technological point of view, developing a robust and stable enough app for the iOS and Android platforms, which are predominant ones in Japan and Europe respectively, has been very tricky. Despite the efforts of Keio University to develop the app and Santander City Council to provide its support in testing, improving and translating the app, the current version is quite slow, the Timeline window takes a long time to display the available posts.
- From a language point of view, the idea of exchanging posts, including pictures and text, between the two continents with the aim of fostering closeness between both cities has encountered a language limitation. In both cities, using English as the common language would have been a barrier to attracting participants to the pilot. Therefore, a Spanish-Japanese and vice versa translation functionality was required. This





translation functionality has been implemented on a first level, when a user makes a post with a caption, the caption text can be translated, from Japanese to Spanish and vice versa. However, when other users make comments, these texts are displayed in the language of the user adding the comment. This is illustrated in the following figure.

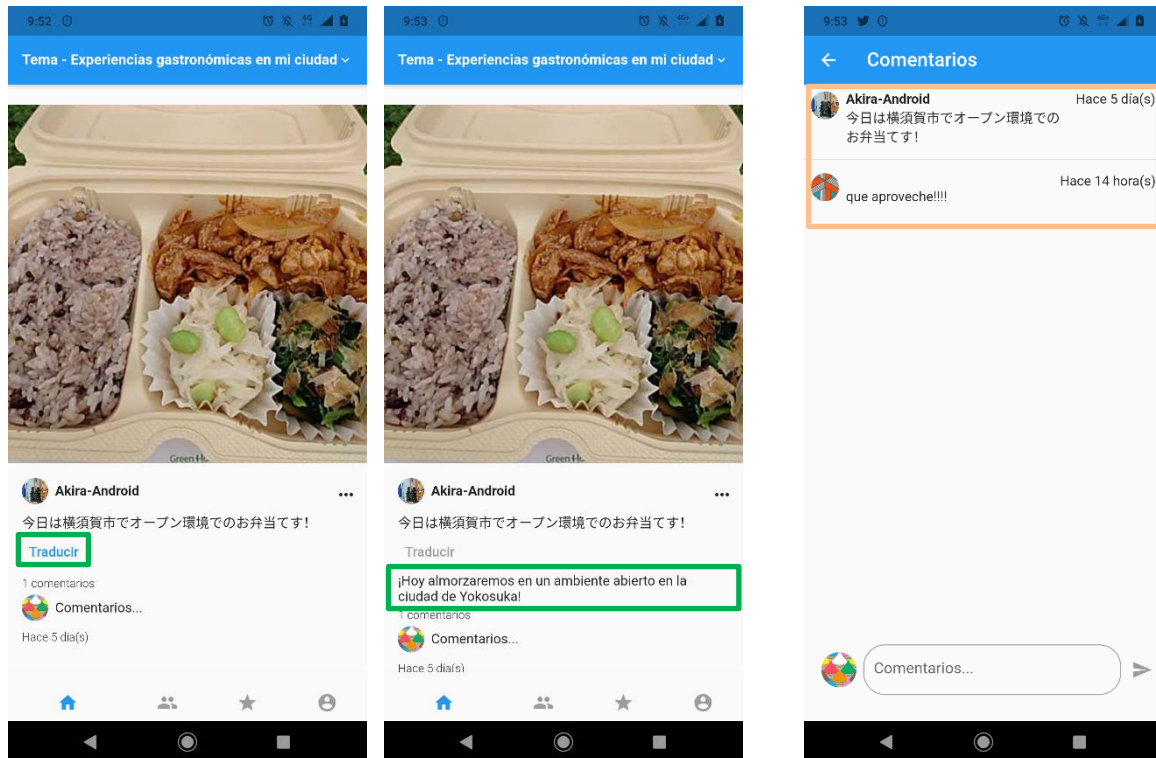


Figure 2—47: Translation functionality available on the 1st level (left side), but not on the 2nd (right side)

Based on the limitations described above and bearing in mind the limited time and resources available, it was agreed to reduce the scope of the cross-border pilot in the case of the city of Santander by involving a group of friend-users in this pilot. 20 user friends have been invited to publish posts on the two available themes, “The most beautiful views of my city” and “Gastronomic experiences in my city” and also to get the 3,000 points that would enable them to complete the pilot questionnaire. This cross-border experience, phase3, started on 21st September and lasted one week, where people from Fujisawa and Santander used SCR app to provide posts on both themes previously mentioned.

In phase3, we applied the following 2 default themes in both cities:





Icon	Default Theme	Explanation
	[Preserved version] Share with everyone · Superb view of this city	Show off our city with beaches, parks and gardens, sunset / night views, iconic buildings ... and your favorite spots! And your smile too.
	Takeaway gourmet pride	Let's brag about home-cooked food, delivery, and delivery gourmet! In addition to the impactful photos, your smile before eating.

Figure 2—48: SmileCityReport Themes for UC4 pilot PHASE3

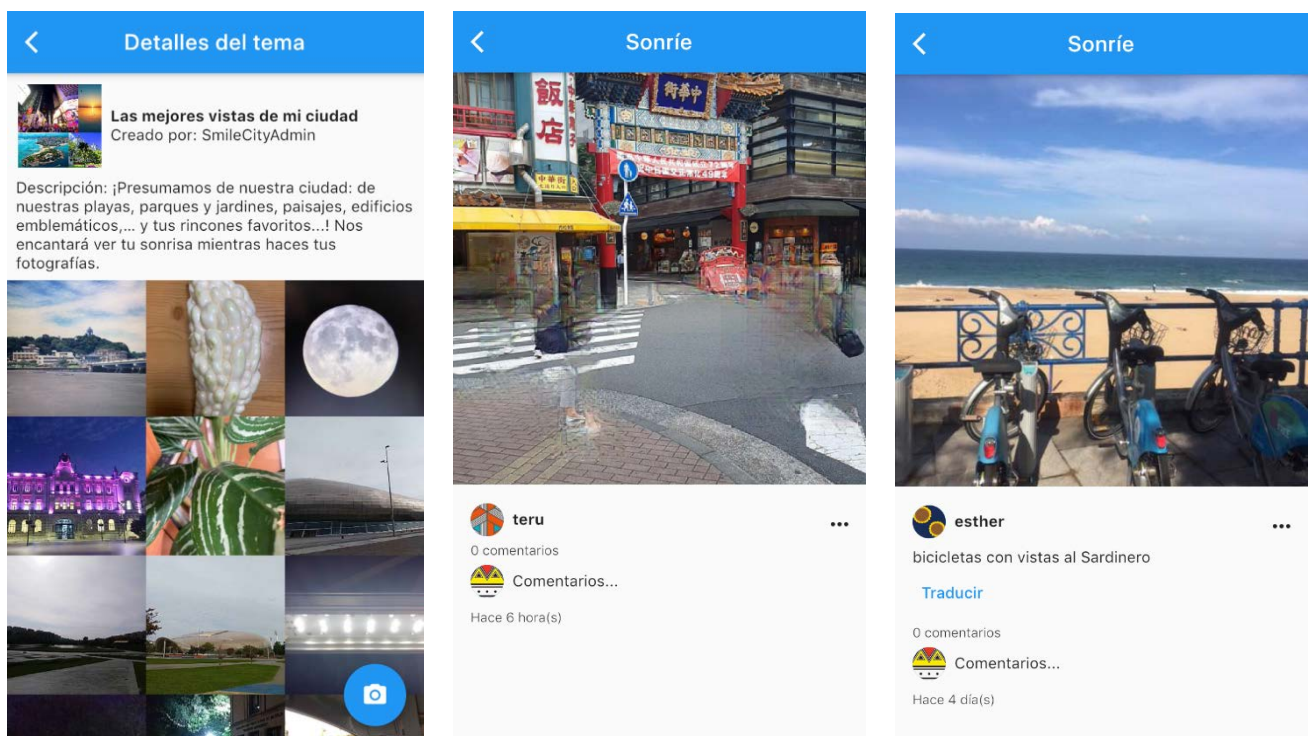


Figure 2—49: Users' post from "The most beautiful views of my city" theme PHASE3



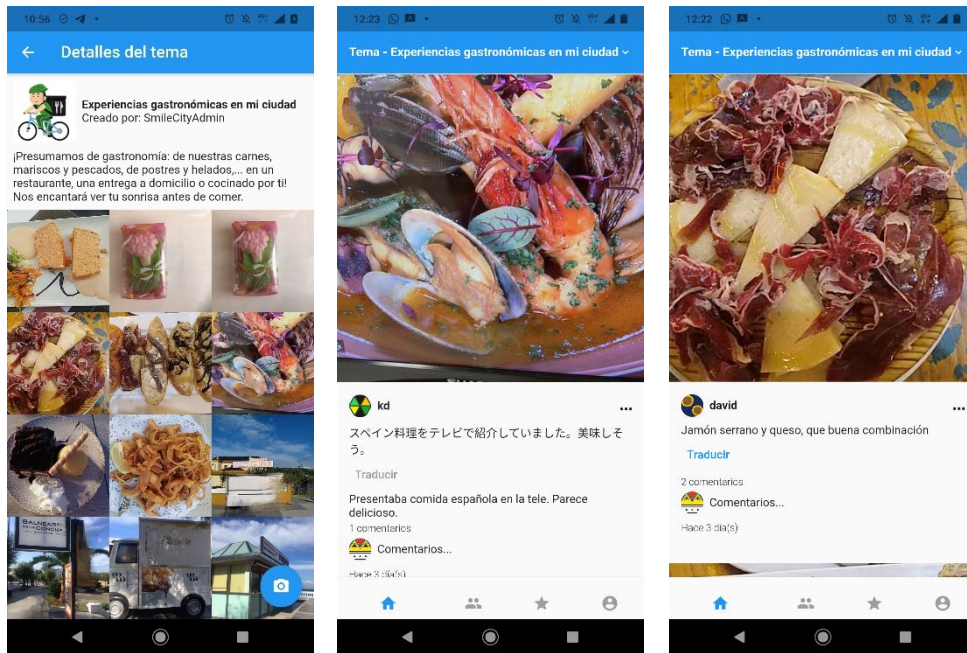


Figure 2—50: Users' post from "Gastronomic experiences in my city" theme PHASE3

In PHASE3, we have collected users' posts statistics as follows:

Table 2-20: Actual number of reports by user in PHASE 3

Theme	# of posts		# of CROSS comments		# of GANonymizer	
	Santander	Fujisawa	Santander	Fujisawa	Santander	Fujisawa
Beautiful spot of the city	61	52	3	31	9	4
Recommended gourmet	9	4	4	8	1	0
Sub Total	70	56	7	39	10	4
Total	126		46		14	

PHASE 3 Participants: 40 (Santander 20 / Fujisawa 20)

In UC4, Pilot PHASE3 conducted in September 2021, was conducted as a cross-border pilot by Santander and Fujisawa City. Although it was still a COVID-19 period, it was carried out with 20 participants each city, for a total of 40 participants. We focused on two themes in particular, but 46 cross-comments were posted for each post in Santander and Fujisawa. As in PHASE2, it was conducted in a COVID-19 environment, with few pictures of citizens and few posts using the GANonymizer tool, as happened in PHASE1.



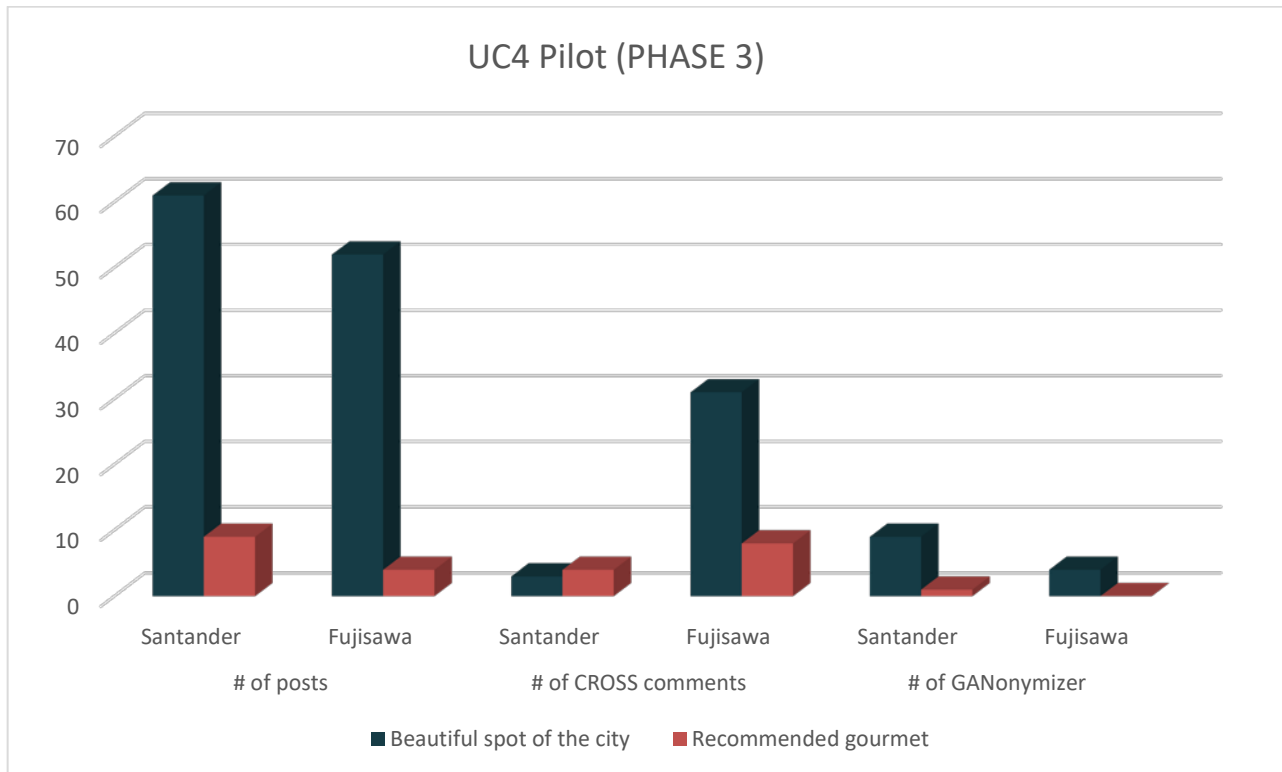


Figure 2—51: Results of UC4 Pilot (PHASE 3)

Pilot dissemination for replication purposes has been done in parallel since the initiation of the pilot in August 2020. Some of the actions conducted are:

- Use Case Blogpost where use case description is showed, including the challenge it addresses, the M-Sec specific approach, the pilot implementation and results as well as the value proposition and the business model canvas. Available [here](#).
- UC Brochure where the unique value proposition is detailed as well as the main stakeholders interested in such a solution, features provided and pilot testimonies. Available [here](#).
- UC Video as a demonstration of the solution and the M-Sec value added. Available [here](#).





Figure 2—52: Pilot4 Blogpost and Brochure



Figure 2—53: Pilot4 Video

In addition to this, Santander municipal website offers a specific section of the M-sec project, providing information about the project and the pilots oriented to end-users including: a detailed pilot description as well as pilot4 video with Spanish subtitles. This can be seen in the following figure and it is available [here](#).





Piloto4: Sensado participativo afectivo seguro de eventos en la ciudad

Este piloto explora la posibilidad de compartir de forma segura información de la ciudad e información afectiva de los ciudadanos. A través de una plataforma de sensado participativo móvil con protección de la privacidad y una aplicación móvil "SmileCityReport" los ciudadanos pueden compartir de forma segura fotos de eventos en la ciudad (por ejemplo, una hermosa flor floreciendo, un lugar turístico de la ciudad, un delicioso menú, un bonito atardecer, etc.) y su información afectiva. La aplicación captura simultáneamente la foto del evento y la cara del usuario mediante el uso de dos cámaras del móvil, cámara trasera y frontal, respectivamente. Dentro de la "comunidad" de usuarios de la aplicación, éstos pueden compartir sus fotos (tanto del evento como de la cara) de manera segura. Adicionalmente, se asegura la compartición de fotos de eventos de la ciudad y datos afectivos protegidos por la privacidad en la red pública (la cara del usuario no es accesible fuera de la "comunidad", sin embargo sí lo es el porcentaje de sonrisa del usuario que ha tomado la foto aportando un valor añadido a la fotografía del evento).

video del

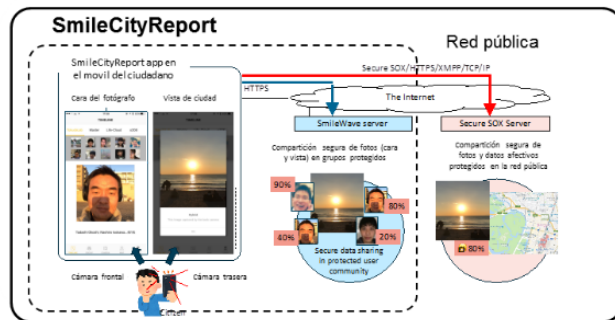


Ilustración del piloto4

Una primera fase de este piloto se desarrolló en la ciudad de Fujisawa, en noviembre de 2020; y una segunda fase se desarrollará en los próximos meses de forma simultánea en ambas ciudades, Santander y Fujisawa.

En este enlace podéis acceder al video del piloto4.

¿Qué aporta el proyecto M-Sec? Este piloto también hace uso de la herramienta GANonymizer que permite eliminar automáticamente la información de privacidad de las imágenes, además, los datos procedentes de la app "SmileCityReport" se distribuyen a través de la plataforma segura Secure SOXFire.



M-Sec Use Case 4 - Secure Affective Participatory Sensing of City Events (Spanish subtitles)

Figure 2—54: Pilot4 information at Santander municipal website and video with Spanish subtitles

Data management

Table 2-21: Use Case4 Pilot 4 data management

Type of data	<ul style="list-style-type: none">Photo image data, and text data posted by using smartphone application "SmileCityReport"
Format of data	<ul style="list-style-type: none">Data format exchanging on smartphone application
Data collection	<ul style="list-style-type: none">Collected by end user of smartphone application "SmartCityReport" as participatory sensing
Data storage	<ul style="list-style-type: none">Data stored database on local serverData stored database on Marketplace when user select post to Marketplace

Data protection policies and processes

This UC4 explores the possibility of secure sharing on citizens' affective information and information on the city, by using "SmileCityReport" on the M-Sec platform as mobile participatory sensing, edge-(mobile)-side computation for privacy protection, secure data sharing of sensed information. First from Fujisawa, and next, this was expanded with Santander as a cross border use case.

Table 2-22: Fact sheet for Use-case 4





Data in encrypted database	<p>Photo data: (1) photographer's facial photo, (2)city event's photo</p> <p>Estimated affective data: (1)smile degree of the photographer, (2)smile degree of the photo viewer</p> <p>Other sensor data: Smartphone sensor data such as (1)activity recognition, (2)light sensors, (3)accelerometer, (4)gyroscope, (5)magnetometer etc. etc.</p> <p>Location information: (3)location information of the photo venue</p> <p>User profile: (1)age range, (2)gender, (3)occupation, (4)residential area</p> <p>Network address: (1)IP addresses of the users</p> <p>Survey answer: (1)Survey answer</p>		
Data in blockchain	Anonymized photos (no showing identity of the person).		
Does it involve to process personal data?	Yes	Please, specify which kind of data	<p>Photo data: (1) photographer's facial photo</p> <p>Estimated affective data: (1) smile degree of the photographer, (2) smile degree of the photo viewer</p> <p>Other sensor data: Smartphone sensor data such as (1) activity recognition</p> <p>(1) age range, (2) gender, (3) occupation, (4) residential area</p> <p>Network address: (1) IP addresses of the users</p>
Data Processing	<p>Photo data: (1) photographer's facial photo</p> <ul style="list-style-type: none"> - Details: facial photo of photographers taken by a Smartphone camera. - Justification: To attractive use of SmileCityReport among registered users. - Minimization control: Preparing both 2 types ("facing" and "masking") for each "theme" on SmileCityReport. In case of a "masking" theme, photographer's face will be automatically masked and will not be opened to other users. <p>Photo data:(2) city event's photo</p> <ul style="list-style-type: none"> - Details: photo of the city venue's scene taken by a Smartphone camera. - Justification: To attractive use of SmileCityReport among registered users, and to let the public SOXFire users to know the city event. - Minimization control: Use of Ganonymizer. The photo will be processed with Ganonymizer and possible privacy data will be erased, in best effort manner. <p>3.Environment data</p> <ul style="list-style-type: none"> - Details: Raw sensor data from smartphone sensors - Justification: To attractive the APP use - Minimization controls: No <p>4.User profile:</p> <ul style="list-style-type: none"> - Details: Registered profile data from users themselves, (1) age range, (2) gender, (3) occupation, (4) residential area - Justification: To attractive the APP use - Minimization controls: No 		





Data Retention	From the beginning of the 1 st pilot, to 10 years after the corresponding research output (e.g., a paper) is published.				
In case, there is personal data, please add the following details:					
DPO	AYTOSAN (protecciondedatos@santander.es)	Controller	NTTDMC	Processor	Keio University

Measures to comply with Privacy strategy on APPI

Acquisition and use of personal information

- In UC4, citizens participate through the smartphone application SmileCityReport, and the users who confirmed the informed consent when installing this application on the smartphone are participating.

Personal data security control measures

- Development of organizational structure is defined in the previous section.
- In UC4, citizens participate through the SmileCityReport smartphone application as described above. So whether it includes privacy contents or not depends on user's photo contents same as general SNS applications. But we solved this issue by using "GANonymizer" which automatically erase privacy data.

Human safety control measures

- Instruction guide of users who are interested in the installation of SmileCityReport

Physical safety control measures

- All data exchanged on M-Sec Secure platform environment same as other UCs

Technical safety control measures

- We provide "GANonymizer" In order to avoid infringement of portrait rights due to the reflection of ordinary citizens in the photos posted by users, users can use the capabilities of automatically erasing privacy related data in the photo by "GANonymizer".

Provision of personal information to third parties in Japan and overseas

- Described in Cross Border Extension section

Supplementary rule: Expanding the range of retained personal data

- There is no additional rule.

Cross-border extension

Several privacy issues arose when considering this cross-border pilot between the cities of Santander and Fujisawa, which were beyond the M-Sec consortium's expertise. The European partner in charge of privacy





tasks, CEA, consulted an external expert regarding this cross-border pilot where a phone application, SmileCityReport, that will be published by a Japanese university, Keio University, that collects a photo and processes it on its servers in Japan. This application will be also offered in the city of Santander in Spain and explicit consent will be obtained.

The external expert indicated that the DPO intervening in this case must be the DPO of the data controller:

- In this case, insofar as the Japanese university publishes and hosts the application, it is understood that the university alone defines the purposes and the means of data processing linked to this application.
- The Japanese university therefore seems here to be qualified as data controller. So indeed, the role of the Japanese university is predominant.
- Japanese organizations are under no obligation to appoint "DPO" which remains a European obligation. However, when Japanese organizations process the data of persons located in the territory of the European Union, they have the obligation to appoint a representative (article 27 of the GDPR) except when the organization is a public authority or a public body. This representative must be "established in one of the Member States in which there are natural persons whose personal data are processed in connection with the supply of goods or services, or whose behaviour is subject to the subject to monitoring "(Article 27, 3. of the GDPR).

Therefore, the Japanese University seems subject to the obligation to appoint a representative in accordance with Article 27 of the GDPR (unless it is qualified as a public body - which it must determine according to Japanese rules in the material). The representative must be appointed in Spain insofar as the application will be offered in Spain.

Following the external expert's response, the next step was to look for this representative, which could be a lawyer firm, although there are more options available (defined in Art 27 of GDPR). The restriction is that the designated DPO must be established in the country where the citizen providing the data lives in. Therefore, taking into account that appointing a lawyer in Spain could be very expensive and also time-consuming, as well as, the pilot will take place in Santander, Santander Municipality could be this representative.

Based on a template for an agreement related to the DPO designation provided by VeraSafe, a representative agreement between Keiko University and Santander City Council adapted to this cross-border pilot was elaborated and signed on 14th May 2021. This document is available in Annex1.

Alongside this representative agreement, the Informed consent for EU citizens to be shown in the Spanish version of the SmileCityReport app was elaborated by Santander Municipality using the draft provided by Keio University. This informed consent follows the multi-layer information approach recommended by the Data Protection Authorities⁶ and applied in UC1 & UC2, as explained in D5.11, section 5.1. The following figure shows the English version of the informed consent, where basic information such as "Controller", "Purpose", "Legitimacy", "Recipients" and "Rights" is provided (at first layer), and also a web link that will lead to the additional information is available in detail (at second layer).

⁶ <https://www.aepd.es/sites/default/files/2019-09/guia-modelo-clausula-informativa.pdf>





INFORMED CONSENT FOR EU CITIZENS

I AUTHORIZE Santander City Council to process my data within the framework of the EU-JP Project M-Sec and on the basis of the following information provided:

BASIC INFORMATION ON PROTECTING YOUR DATA	
Controller	Santander city council
Purpose	Participating in the cross-border pilot "Share your experiences in the city through the SmileCityReport app", within the framework of the EU-JP M-Sec Project, which the effectiveness of participatory sensing that can share "events in the city" and "the emotional state of the user who reported it" while protecting the user's privacy.
Legitimacy	Consent of the interested party and Mission in the Public Interest
Recipients	The personal data collected will be sent to Keio University, which will anonymise the data.
Rights	Access, rectification, erasure, restriction of processing and, where appropriate, objection and portability of data.
Source	Those provided by the participants in the registration process and use of the "SmileCityReport App"

For additional information regarding the protection of your data, please consult the following web link:
<http://santander.es/ayuntamiento/proteccion-datos/informacion-adicional-proteccion-datos>

Figure 2—55: Informed consent for EU citizens (English version)

Finally, several actions were taken to ensure that the SmileCityReport app is GDPR compliant:

- Privacy policy in iOS & Android Markets: When accessing both markets, iOS & Android, to download and install the Smile City Report app, in the "privacy policy" section in the case of European users, a link to the privacy policy of Santander City Council should appear. In the case of Japanese users, a link to the privacy policy of the University of Keio should appear, as can be seen in the following figures.



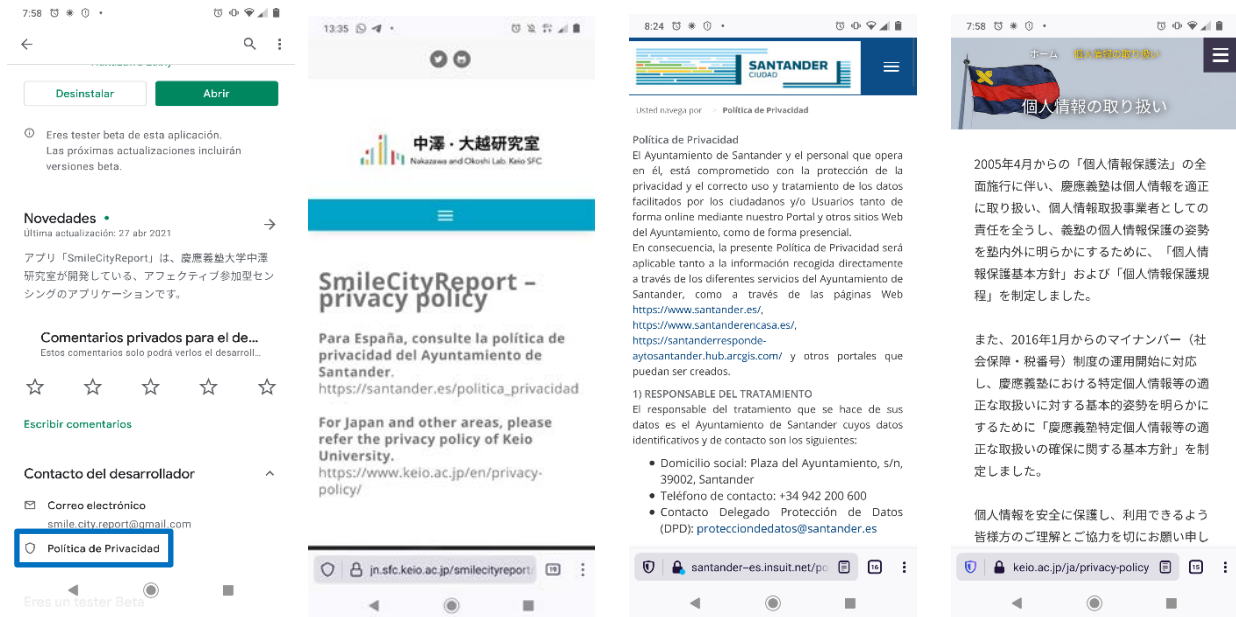


Figure 2—56: Privacy Policy in Markets: EU side and Japanese side

- Informed consent is shown once SmileCityReport app has been installed by the user, and only when she/he accepts its terms, she/he is able to register and start using the app.

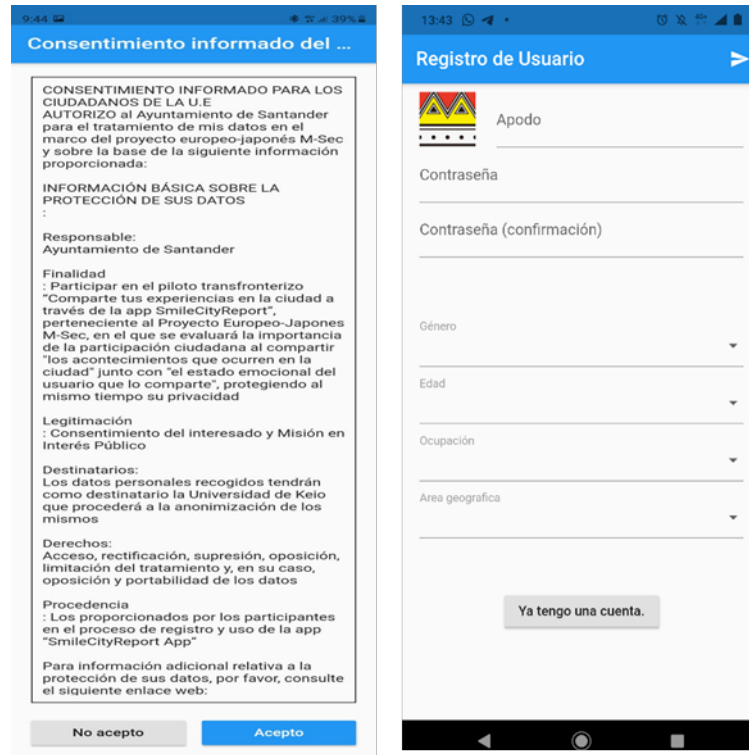


Figure 2—57: Spanish version of the Informed Consent to be accepted before registration phase





Technical approach – M-Sec components

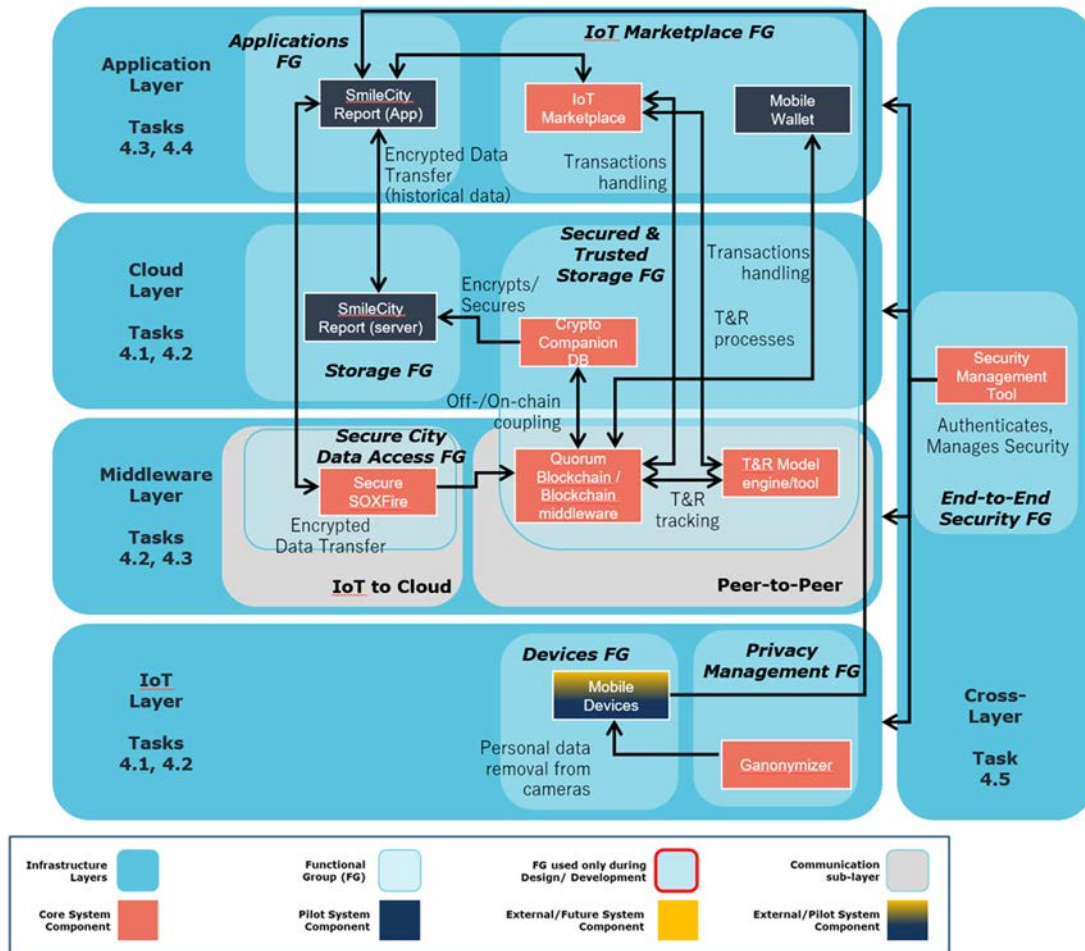


Figure 2—58: Use Case 4 Architecture View

UC4 uses SmileCityReport to provide a secure, participatory sensing platform for citizen events. Furthermore, we aim to become a cross-border pilot in collaboration with Santander from Fujisawa City this time. In order to realize these, M-Sec's Marketplace function is combined with the SmileCityReport environment that can be linked globally under the multi-layer security mechanism of M-Sec.

From the privacy protection view point, UC4 implements "GANonymizer" tool that automatically erases privacy-related information from images taken with the mobile phone's front camera, by image processing using deep learning. Below some examples of pictures before and after applying the "GANonymizer" tool are shown.



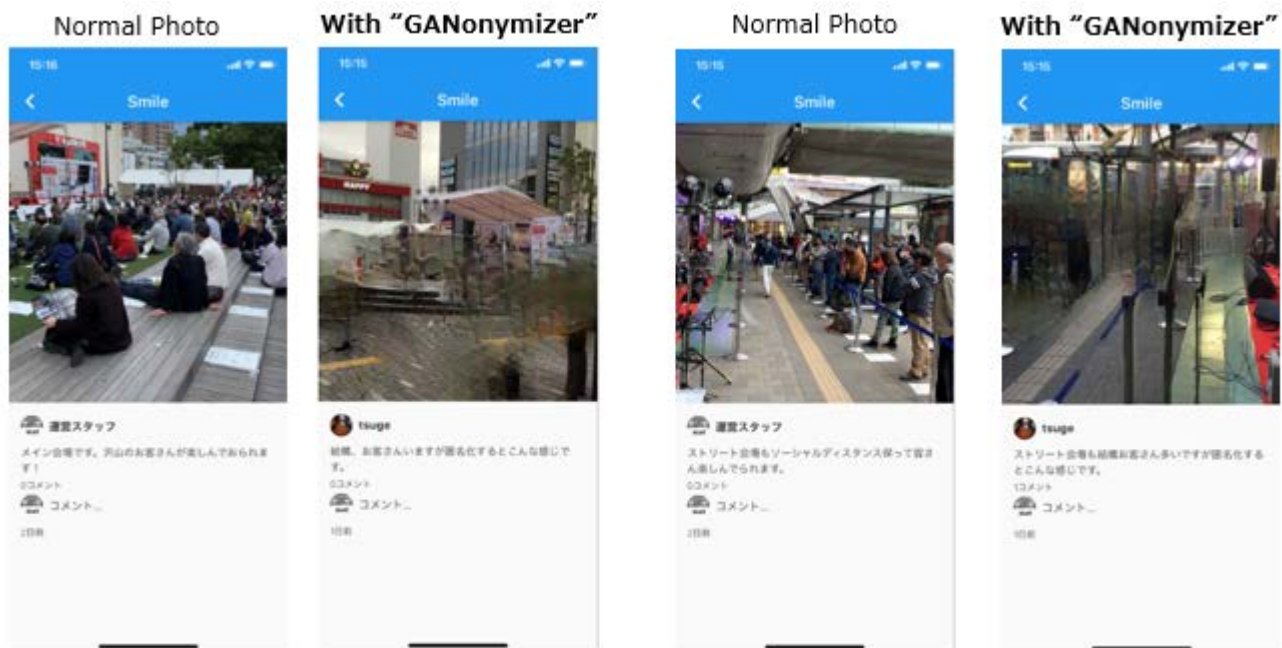


Figure 2—59: Automatically Privacy Data Protection by GANonymizer

Pilot setup

Table 2-23: Use Case4 set up

Planning	<ul style="list-style-type: none">● Start Date: M28 (November 2020)● Duration: M28 – M39 (11 months)● Phases:<ul style="list-style-type: none">○ PHASE 1 – Fujisawa City Event (M28): The 1st UC4 actual pilot at “Fujisawa Jazz Meetin 2020” on 7th November 2020○ PHASE 2 – Fujisawa City Pre-Final Trial (M36 – M37): Pre-Final pilot in Fujisawa city by 260 user participants○ PHASE 3 – Cross Border Trial with Santander (M39): Final pilot as actual cross border pilot EU and Japan
Pilot set-up	<ul style="list-style-type: none">● Prepare and test smartphone Application “SmileCityReport” which is compatible for both iPhone and Android● Setup Informed Consent for confirmation to end users of Santander and Fujisawa● Prepare quick manual for citizens in Fujisawa● Setup event booth at Fujisawa Jazz Meeting 2020 event● Prepare Questionnaire in order to evaluate in each phase (English, Japanese & Spanish versions)





KPIs

The table below shows the current updates to the initial KPI goals, including the above results.

Table 2-24: Use Case4 Pilot 4 KPIs

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

Questionnaires

In order to evaluate the level of satisfaction of the participants in this cross-border experience, the Smile City Report app includes a link to a questionnaire in google form: a pop-up message appears when the user has accumulated 3,000 points through their posts and comments. This survey is available in Japanese for Fujisawa participants and in Spanish for Santander participants, which has been very used full for getting participant's feedback.

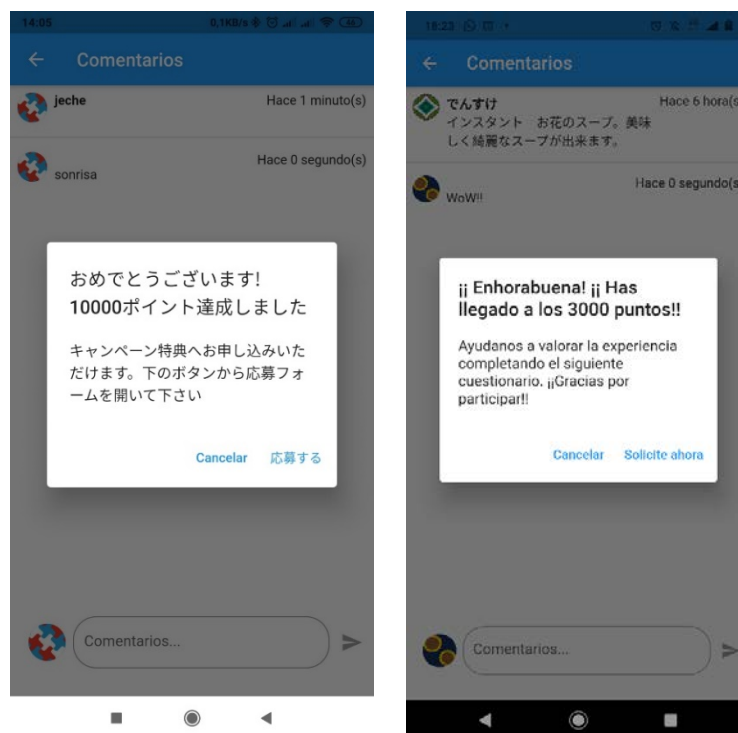


Figure 2—60: Japanese & Spanish version of the pop-up questionnaire message





The English version of this questionnaires is shown below and results from this survey can be found in D2.8 M-Sec validation and overall evaluation.

M-Sec e-Survey_Crossborder UC4

M-Sec is a Research and Innovation EU-Japan collaborative project. Its main goal is to develop an innovative solution that ensures a more secure (and less vulnerable) data transfer between stakeholders (such as citizens, researchers, companies, local municipalities) when using IoT devices and applications in hyper-connected smart cities.

In the scope of this research, the project is now conducting an online survey to all EU and Japanese citizens and stakeholders, considered as potential users of the M-Sec solution, to collect feedback on their IoT devices and applications experience and on their knowledge of EU and Japan's data protection regulations.

Filling in this survey will not take you more than 1 minute. Help us further understand the IoT ecosystem in which M-Sec is expected to operate.

For more information on the M-Sec project, please access <https://www.msecproject.eu/>

Thank you so much for your collaboration,

The M-Sec Team

Your background

The information contained in this survey will be treated anonymously and presented in an aggregated way.

Email Address

Your email will be used by M-Sec only if you accept to receive more information about the project, such as Webinar invitations, etc. Apart from that, it only intends to send you a notification email upon completion.

At the time of this reply, I represent...

- *a citizen*
- *a member of a private company*
- *a municipal officer*
- *a developer*
- *a researcher at a University and/or a research centre*
- *Other:*

Your IoT security and privacy concerns

As individuals, we currently use more than 1 IoT device. Therefore, we would like to better understand if you have any concerns, and what those might be, regarding the security and privacy of your personal information when using those devices.

Are you aware of security and privacy data protection policies when using a given IoT device or application?

- *I am fully aware (i.e. I always read carefully the data protection policies when using a given device or application)*
- *I am not that fully aware (i.e. I do not always carefully read the data protection policies when using a given IoT device or application)*
- *I am not aware (i.e. I never read and always accept the data protection policies when using a given IoT device or application)*

What are your concerns when you hear about a cyber-attack in a given IoT device or application that you are currently using?

- *I go and check carefully the data protection policies when using the IoT device or application*
- *I stop using that specific IoT device or application*





- Other:

What are your concerns when using IoT devices or applications?

- Theft of personal data
- Use of your data by others
- Mistrust in the results of the measured data
- Ownership of the data
- Difficulty in the use of devices or applications
- Other:

Your awareness of data protection policies

As this is a mandatory question, if you have answered No in the previous question, please also answer No in this one.

Are you aware of your rights regarding EU's General Data Protection Regulation (GDPR)?

- No, as I am not from an EU country
- Yes, I am completely aware
- I have heard about it but I am not completely aware of my rights
- No

Are you aware of your rights regarding Japan's Act on the Protection of Personal Information (APPI)?

- No, as I am not a Japanese citizen
- Yes, I am completely aware
- I have heard about it but I am not completely aware of my rights
- No

Regarding SmileCityReport

*How did you like smart city report? **

From (1) Not satisfied at all to (5) Very satisfied

*Were there any post that are valuable for you? **

From (1) Not at all to (5) Many

*How was the app that "posts according to the theme" about the current state of the city? Do you want to use this app again? **

- I would like to use it again very much.
- I would like to use it again.
- I am not sure.
- I do not want to use it.
- I do not want to use it at all.

*How was the function to take pictures of the scenery and yourself at the same time with the two cameras on your smartphone? **

- Very interesting
- Interesting
- I am not sure
- Not interesting
- Not interesting at all

*How did you know this app? **





- Flyer
- M-Sec Project Website
- Friends
- Otro:

Regarding privacy protection tool GANonimizer

*Did you use a privacy protection tool called "GaNoymizer" in the app? It is an AI technology to erase the reflected "parts that may contain privacy information" in the picture such as people. **

- Yes
- No

*How did you think about the tool? **

- Very valuable
- Valuable
- I am not sure
- Not Valuable
- Not Valuable at all

*Did the privacy protection tool properly remove the "parts that would contain privacy information" from the photo, such as people? **

- It worked very well.
- It worked.
- I am not sure.
- It did not work.
- It did not work at all.

Summary – lessons learned, sustainability

UC4 Pilot was conducted based on participatory sensing using the smartphone application "SmileCityReport". Based on the secure smart city platform provided by M-Sec project, citizens of Santander and Fujisawa have actually participated in a "Cross Border Citizen-participatory pilot", thus illustrating the Japan-Europe collaboration of the M-Sec project.

UC4 has been carried out step-by-step with three PHASEs to concretely realize this challenging Pilot requirement. In the 2nd year of the project, the world was already in the harsh environment of COVID-19, but at the citizen Jazz event "Fujisawa Jazz Meetin' " held in Fujisawa City, the demonstration using the smartphone application "Smile City Report" for the first time was carried out as PHASE1. And in the final 3rd year of the project, under the environment of COVID-19 deteriorated further, but as PHASE2, 1,340 posts were posted from 250 participants while participating completely online in Fujisawa City. And in the final stage, PHASE 3, we realized a cross-border Pilot with a total of 40 participants from each of Santander and Fujisawa. Of particular note is that the 46 cross-border posts were exchanged between Santander and Fujisawa, even if under their limited translation capabilities, and even if they didn't understand each other's languages.





Actually, there were restrictions due to the difficulty of maintaining a certain level of quality on many Android models in addition to the iPhone and the limited translation function, but toward future development, it was a very good reference.





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

Pilot scenario and objectives

This pilot is a cross-border trial, implemented in Santander and Fujisawa. The M-Sec data marketplace is set up for citizens, companies and municipalities to trade data collected in other use cases and valuable datasets on the internet 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 to make the data effective enough to contribute to “build” a 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. The initial approach of this Marketplace includes data coming from M-Sec pilots, city data from Santander Open Data Platform as well as pictures uploaded by Marketplace users', including also SCR app users'. In more detail users are able to browse the IoT Marketplace, view M-Sec and user generated data descriptions and purchase from the following tabs in the Front End:

- Sensor data coming from different sensors as part of use cases
- Photos uploaded from other users with details such as description, price, title, tag
- Photos from smile city report application
- Sensor data from SOXFire sensors, arriving to the IoT Marketplace via the IoT Marketplace-SOXFire Bridge
- Datasets from Santander Open Data Platform by utilizing the related API

For all the sensor data, there is a description of its type and proposed units of measurement as shown in the following table:

Table 2-25: Detail of sensor data available in M-Sec Marketplace

Code	Type of sensor	Proposed unit of measurement
1	Temperature	°C
2	Relative humidity	%
3	Pressure	hecto Pascal – hPa
4	Visibility	Km





Code	Type of sensor	Proposed unit of measurement
5	Wind speed and direction	m/s°
6	Sky cloud coverage	%
7	Dew point	°C
8	Solar Radiation	watt/m ²
9	UV index	0 to 11
10	Columnar density of total atmospheric ozone layer	Dobson – DU
11	Motion sensors	Int [0,..]
12	Door window	Int [0,..]
13	Smart Plug	Volts
14	Smoke	Bool (on/off)
15	Mattress	Bool (on/off)

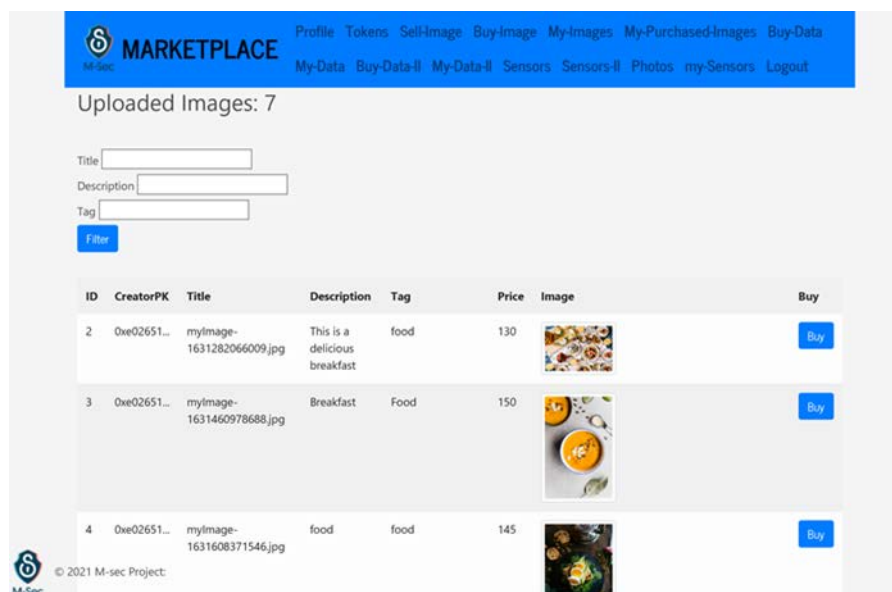


Figure 2—61: Marketplace Initial User Interface





Challenges and mitigation actions on pandemic situation

Table 2-26: Use Case5 Pilot 5 Challenges & Mitigation actions.

Number	Challenge	Mitigation Action
1	The collaboration events were cancelled or postponed due to the COVID situation.	Setup a long-term field trial period instead of one-off.
2	Not to get in touch with event organizers(stakeholder)	Setup meetings periodically to come up with other ideas for field trials.
3	Low number of participants	Provide tokens for free. Organize a workshop to present M-sec Market Place to more tech-savvy profiles (universities, research centres, ...)
4	Not enough data available on the marketplace	Once data from all UCs is integrated on the marketplace, it will be assessed if more data is needed.
5	Leak of personal data transferred to the MarketPlace	Registration data: there is not risk of leak of data. No risk related to Data stored/exchanged on marketplace (off-chain). The integration of IoT Marketplace with Security Manager ensures that no leak of personal data is feasible since an anonymisation process is followed. Additionally, no personal data are stored in the Marketplace
6	Control data uploaded by stakeholders	Technically it is possible to add control. The exposed API and implementation of the IoT Marketplace allows the “freezing” of users activity or not allowing specific sensor data to be purchased. The latter is feasible only for the owner of the specific sensors. Both these methods allow the control of specific users and sensors data.

Engagement process with citizens and stakeholders

Marketplace participants are the data buyers and data providers who need/can provide specific data. Expected participants are citizens, municipalities, companies, research institutions, etc. As it is a digital platform, they will need a certain level of IT literacy and devices such as computers or smartphones with network environment to exchange data. Thus, we have requested cooperation from M-Sec stakeholders to try it out through the webinars and M-Sec page. In addition, we have also asked UC4 participants, which counts of about 200 users, to cooperate by introducing the data marketplace at the same time as trying out the Smile City Report as UC4 is relatively easier to reach to participants and the marketplace can be accessed from the





Smile City Report application, so the participants can exchange their pictures posted and buy the pictures that they like in the marketplace through the Smile City Report application. Additionally, more tech-savvy users have been invited to join the M-Sec Marketplace, and buy not only pictures but also data coming from the different M-Sec pilots.

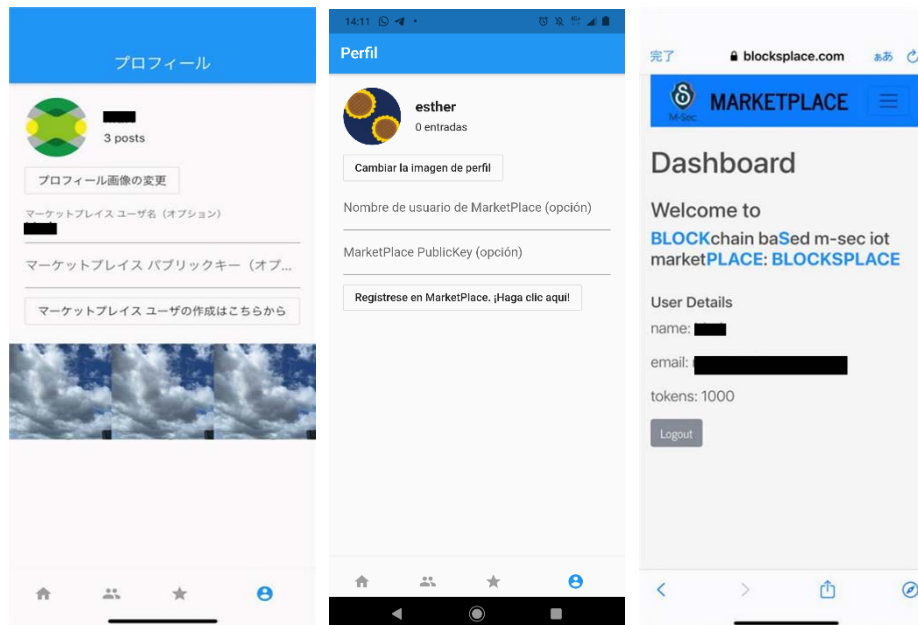


Figure 2—62: Marketplace Interface from Smile City Report app and Marketplace Dashboard on Smartphones

Some of the consortium dissemination actions conducted are:

- Use Case Blogpost where use case description is showed, including the main challenges it addresses, the M-Sec approach, the pilot implementation and outcomes together with the value proposition and the business model canvas. Available [here](#).
- UC Video as a demonstration of the solution and the M-Sec value added. Available [here](#) with English subtitles, and [here](#) with Japanese subtitles.
- UC Brochure where the unique value proposition is detailed as well as the main stakeholders interested on such a solution, features provided and pilot testimonies. Available [here](#).
- Additionally, a dedicated online seminar, “IoT Marketplace for secure hyper-connected city data: official launching of the M-Sec Project Marketplace”, was held on 8th July 2021 to present the M-Sec Marketplace and attract participants to join this pilot. The recorded webinar is available [here](#).





USE CASE 5 - SMART CITY DATA MARKETPLACE WITH SECURE MULTI-LAYER TECHNOLOGIES

Fujisawa & Santander

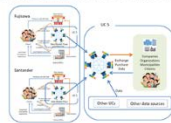
This UC5 is to build an M-Sec marketplace where data collected during field trials in each use case can be traded in both Japan and Europe while ensuring security on all layers through blockchain and other mechanisms.

Problem Overview:

This UC will handle all sorts of data including personal data which needs to be prevented from falsification and be traded in a secure environment and need to avoid attacks to the blockchain and the actual marketplace.

Stakeholders:

- **Citizens:** sharing personal information (location, preferences) using the points/coupons system
- **Universities and Research Institutions:** not confirmed yet
- **Citysec:** in case the municipality or agent in participation is responsible for the management of a festival/event (the "Charm" event)
- **Companies:** businesses in event urban special events take place, which will accept the coupons from citizens and may organize competition/games/promotional events for their businesses through "Seeds City Report".



GDPR compliance:

DATE: 25/09/2018

CATEGORY: use cases

SHARE: f t g+ in t @

Figure 2—63: Use Case 5 Blogpost



Figure 2—64: Use Case 5 Videos in English & Japanese



Figure 2—65: Use Case 5 Brochure





As mentioned in previous pilots, the Santander municipal website offers a specific section for the M-sec project, providing information about the project and the pilots oriented to end-users including: a detailed pilot description as well as pilot5 video with Spanish subtitles. This can be seen in the following figure and it is available [here](#).

Piloto5: Mercado de datos seguro con tecnologías multicapa

El objetivo de este piloto es construir un mercado M-Sec en el que los datos recogidos en los pilotos desarrollados en el proyecto puedan intercambiarse tanto en Japón como en Europa, asegurando la confidencialidad, integridad, disponibilidad y privacidad de los datos, garantizando la seguridad en todos los niveles mediante blockchain y otros mecanismos. Adicionalmente, este mercado de datos se abrirá a agentes externos al proyecto para que puedan acceder a aquellos datos que les resulten interesantes.

Ilustración del piloto5

Se están ultimando los detalles de este piloto que se pondrá en funcionamiento en los próximos meses. En el siguiente enlace podéis acceder al video del piloto5.

¿Qué aporta el proyecto M-Sec? El mercado necesita gestionarse en un entorno seguro, teniendo en cuenta los requisitos de seguridad y privacidad de GDPR y APPI. Además, M-Sec ha investigado en profundidad el hecho de combinar la base de datos encriptada y el blockchain, lo que mejora considerablemente la seguridad, al tiempo que garantiza la fiabilidad de los datos y la privacidad de los usuarios. También integra un sistema de confianza y reputación dentro de la implementación del blockchain.

INTERCAMBIO DE DATOS

BASE DE DATOS ENCRYPTADA

MERCADO DE DATOS M-SEC

DATOS ANONIMIZADOS

YouTube

MARKETPLACE

Purchased Image 1

Si queremos comprar alguna, sólo tenemos que hacer click en "Comprar" y accederemos a una lista con todas las imágenes que hemos comprado.

M-Sec Use Case 5 - Smart City Marketplace With Secure Multi-layer Technologies (Spanish subtitles)

Figure 2—66: Pilot5 information at Santander municipal website and video with Spanish subtitles

In order to increase the number of participants in this pilot, several actions have been implemented:

- Improving the Marketplace user interface, the different functionalities have been regrouped into four categories: Account, Buy, My-Purchased-items and Sell, as can be seen in the next figure. This improvement would be further enhanced by including more detailed and user-friendly information on the data available in the Marketplace.
- Tokens button, when a user registers on the M-Sec Marketplace, she/he gets 1000 M-Sec tokens, which she/he can use to make purchases. The number of tokens can be increased by 100 tokens by clicking on "Tokens" button, included in the Account category.



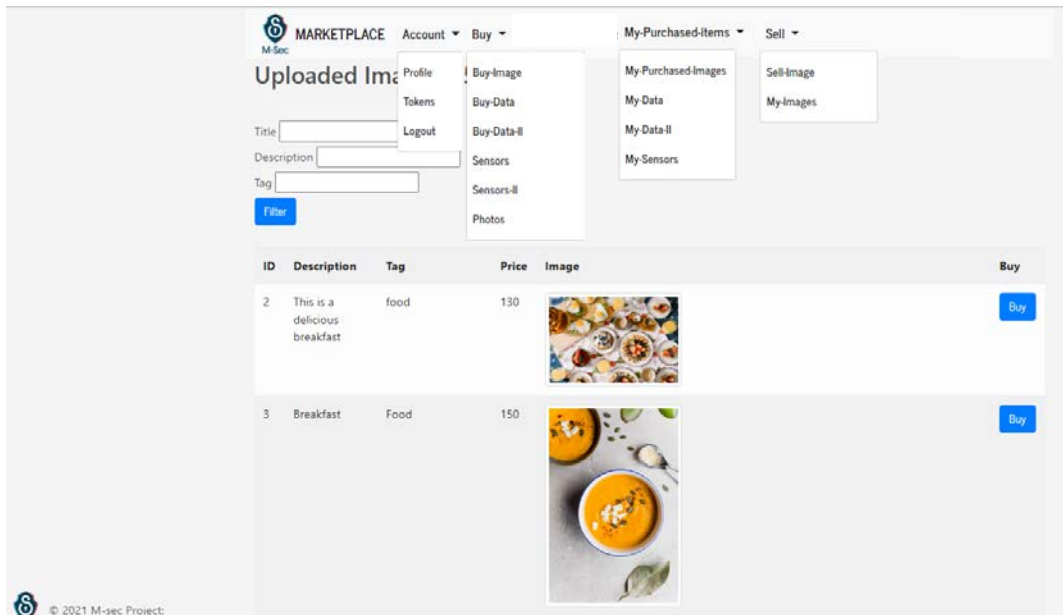


Figure 2—67: New Marketplace User Interface

Data management

In the context of UC5, data from different UCs are available to view, exchange and purchase mainly through the IoT Marketplace. So, this sub-section includes all the information provided in corresponding sections “Data Management” of previous Use Cases and to avoid replication is not mentioned again. Additionally, users are able to upload/purchase image data accompanied with text data, which are described below.

Table 2-27: Use Case5 Pilot 5 data management

Type of data	• Photo image data, and text data posted by using IoT Marketplace user interface
Format of data	• Data format exchanging on smartphone/Desktop UI
Data collection	• Uploaded by end user of smartphone/Desktop
Data storage	• Decentralized storage on IPFS

Data protection policies and processes

Building an M-Sec marketplace where data collected during field trials in each use case can be traded in both Japan and Europe while ensuring security on all layers through blockchain and other mechanisms.





Table 2-28: Fact sheet for Use-case 5

Data in encrypted database	<p>Personal data needed from users at registry phase to sell and buy in the marketplace (user ID and e-mail address)</p> <p>User profile: All the personal data should be stored here. A UID / pseudonym would also be used here to “link” data stored in the DB with the corresponding data to the blockchain (like an index. That’s part of the integration of the blockchain with the encrypted DB; an ICCS-WLI task).</p>		
Data in blockchain	<p>All the non-personal data from other use-cases blockchains with in addition related to the transactions per se: timestamps, ids (or pseudonyms) of the ones executing the transactions/interactions, ids of the “products” being exchanged, types of transactions and their corresponding virtual value (e.g. points, coupons, virtual currencies, etc.). No personal data will be included in the blockchain, but the corresponding users’ profiles will be linked with the corresponding personal data on the encrypted DB (see previous description on the DB).</p>		
Does it involve to process personal data?	No	Please, specify which kind of data	UserID, E-mail address
Data Processing	<p>1.-City events Photo data which doesn’t include personal information.</p> <ul style="list-style-type: none"> - Details: Photo data handled via - Justification: Share the events data - Minimization controls: No <p>2.Environment data</p> <ul style="list-style-type: none"> - Details: Raw data from smartphone sensors - Justification: To attractive the APP use - Minimization controls: No <p>3.User profile:</p> <ul style="list-style-type: none"> - Details: Registered profile data from users themselves, (1) User ID (2) E-mail address - Justification: To identify the user of marketplace - Minimization controls: No <p>4. Garbage collection activity data</p> <ul style="list-style-type: none"> - Details: Counting data from sensors and video data - Justification: Necessary to monitor the collection activity - Minimization controls: no <p>5. Climate or geography information</p> <ul style="list-style-type: none"> - Details: Raw data from sensors - Justification: measure the climate and geography condition - Minimization controls: No <p>No personal data are stored or processed in the IoT Marketplace.</p>		
Data Retention	<p>From the beginning of the 1st pilot, to 10 years after the corresponding research output (e.g., a paper) is published.</p>		

Measures to comply with Privacy strategy on APPI

Acquisition and use of personal information

- Before register, obtain user agreement that personal information required for user registration will be obtained and it will not be used for anything other than the use of this service.

Personal data security management measures

- In data trading, personal information is not subject to be traded. However, in order to obtain personal information such as user ID and e-mail addresses in user registration, management and operation are performed on an encrypted database from the viewpoint of personal information protection. In the





unlikely event of information leakage, the user will be notified, access from the outside will be blocked, and the operation of the entire marketplace will be suspended.

Human safety management measures

- If there is an update of the Personal Information Protection Law while operating the service, inform people involved in the operation. Also, if necessary, inform the users about the updated contents.

Physical safety control measures

- Since it is not stored in individual electronic devices or servers, it will not be leaked due to physical negligence. If there is a problem with the server, users will be notified of the service outage and the impact it has caused.

Technical safety management measures

- The database is encrypted and can only be accessed by the developer. In addition, access authentication uses two-step authentication using a mobile phone.

Provision of personal information to third parties in Japan and overseas

- This service does not provide personal information to third parties. Therefore, it is not applicable.

Anonymous processing information

- Since data trading is non-personal information, it is not necessary to anonymize it.

Standards for creating anonymously processed information

- Since data trading is non-personal information, it is not necessary to anonymize it.

Supplementary rules

- Since data trading is non-personal information, it is not necessary to anonymize it.

Request for disclosure of retained personal data

When obtaining the consent for user registration, the user will be informed about necessary items (operator, purpose of use, billing procedure and contact information when a problem occurs).

Technical approach – M-Sec components

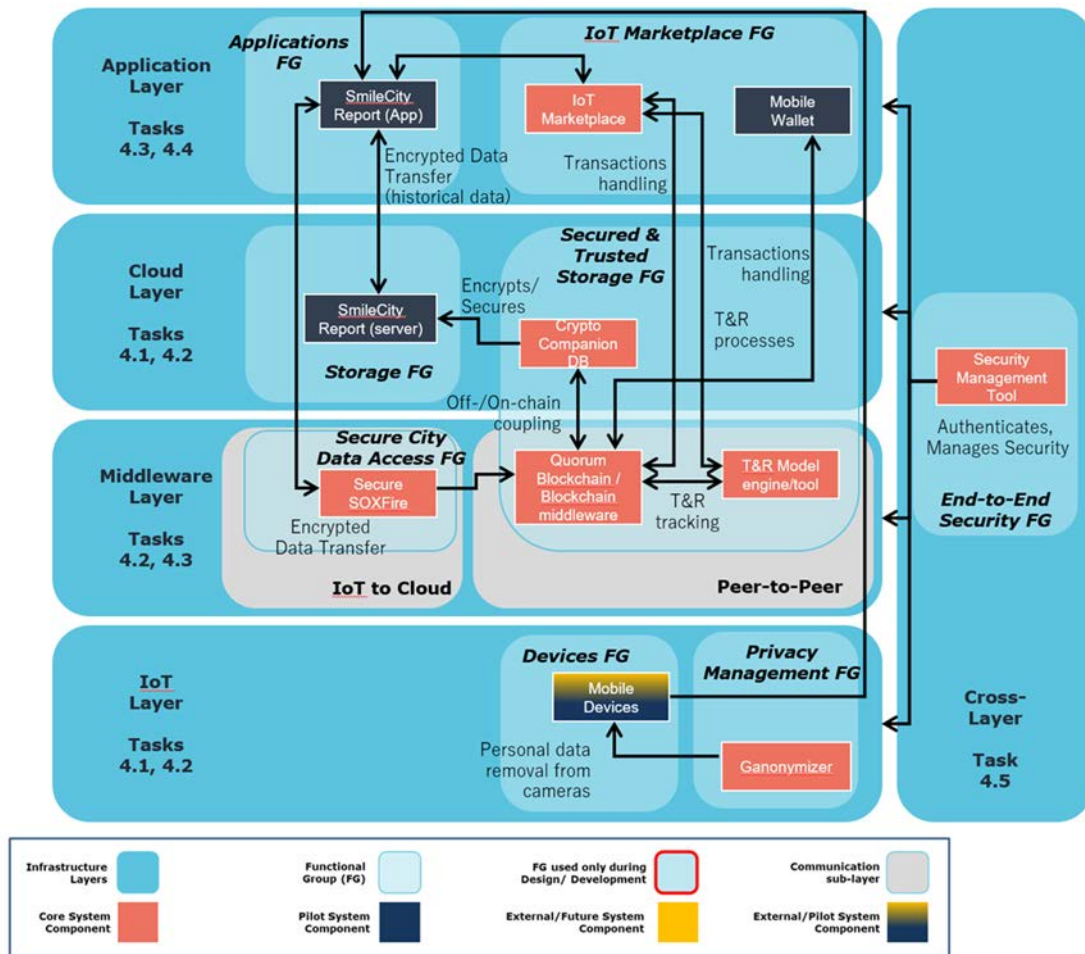
Use Case 5 utilizes the IoT Marketplace to make available data to end users from different use cases and components of the overall M-Sec architecture. Towards this direction, the Integrations among IoT Marketplace FG and other FGs such as Secured & Trusted Storage FG and Secure City Data Access FG had a crucial role.

The technical features, mechanisms and interactions of modules that support the use case are based on the M-Sec architecture, shown in the following Architectural view. The core assets utilized for the purposes of the use case are:





- i) The IoT Marketplace based on Blockchain and the corresponding Middleware:
End users have access to all the services provided by the IoT Marketplace. This way, they are able to register to the platform, upload content, browse and purchase media items etc. Similarly, they can purchase datasets or sensor data, after browsing the related tabs in the Marketplace. Additionally, through the integration with other components more assets are indirectly utilized, as will be described in the next sub-sections.
- ii) The Smile City Report: it is an entry point for the end users and facilitates their interaction with the system



Integrations

In this section, the interactions among the different assets and the technical details are presented. Based on the architecture and the requirements, we proceeded to the implementations facilitating the integrations among different assets. In some cases, new modules were created, for example for the integration of IoT Marketplace and KEIO SOXFire, the “IoT Marketplace – KEIO SOXFire Bridge” was developed. More details about the integration could be found in D2.3 and the main point of integration are:

- Integration between IoT Marketplace & SOXFire
- Integration between IoT Marketplace and Smile City Report Application
- Integration between IoT Marketplace and Quorum Blockchain





Pilot setup

Table 2-29: Use Case5 set up

- Planning**
- **Start Date:** M26 (September 2020)
 - **Duration:** M21 – M39 (15 months)
 - **Phases:**
 - **PHASE 1 – Design of the Pilot** (M21-22):
 - **PHASE 2 –Marketplace development** (M23-M35)
 - **PHASE 3 –Integration with other UC data** (M36-M38)
 - **PHASE 4 – Pilot Evaluation** (M39)

KPIs

Table 2–30. Use Case 5 Pilot 5 KPIs

#KPI	Goal	Target	How to measure?
#of transactions	Get stakeholders involved and motivate them to sell and buy data (or just exchange them)	>10000	Marketplace
# of data resources	Upload data from all the use cases' FT, utilize sensorizer.	>1000	Marketplace Companion Database
# of users	According to the recruitment criteria, we will have webinars, workshops and so on to gather the participants.	>100	Marketplace
# of engaged businesses / organizations (e.g. accepting the coupons system)	Get stakeholders involved and motivated.	>10	Marketplace
% non-malicious entities at the Marketplace	By using permission mechanisms and trust & reputation model.	>51	Marketplace & M-Sec blockchain
Limit of requests from DDoS attacks	Using “gas” for these transactions, thus making an attack that could have exceeded the capabilities of the platform too expensive.	<10.000 (number of transactions per second that the blockchain can handle)	Marketplace & blockchain
% Net promoter scoring	Through a questionnaire, more focused on net promoter score.	>70	Marketplace





Questionnaires

Within the Pilot 5 a questionnaire was prepared to get feedback from users. This questionnaire was implemented through the Google Form service. This questionnaire contains general questions from M-Sec e-survey and Pilot 5 specific questions below:

Section 5 - IoT Marketplace

説明 (省略可)

Do you think that the web is user-friendly? *

	1	2	3	4	5	
I do not like it at all	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	I like it very much

How often do you think you will use the marketplace? *

	1	2	3	4	5	
Never again	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	Very often

Please rate the data available in the marketplace according to your interest. *

	Not interesting	Interesting	Very interesting
Temperature (UC1)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Humidity (UC1)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
CO2 (UC1)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
VOC (Volatile Organic Co...	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Number of visitors (UC1)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Indoors Temperature (U...	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Movement measures (U...	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Electricity consumption (...)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Bed/sofa occupancy (UC...	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Opening doors & window...	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>





Which other data would be interesting for you? Please indicate. *

記述式テキスト（長文回答）

Would you recommend MarketPlace to other users? *

- ☐ Yes
- ☐ Maybe
- ☐ No

Please indicate the reason for the previous question.

記述式テキスト（長文回答）

Summary – lessons learned, sustainability

As discussed at the beginning of the project, UC5 has succeeded in integrating the technology to enable transactions on the secure marketplace in the form of encrypted or anonymized data of other UC1 to UC4. In addition, although it was just before the end of the project period, we were able to validate the marketplace at the user level, albeit on a small scale.

In addition to UC data, we also linked with open data from the city of Santander and open data collected by Secure SOXFire, and implemented of trading various types of data in M-Sec marketplace. The data must be published in an encrypted or anonymized form, but the keyword display, item classification, and menu setting that allow the extracted raw data to be operated without specialized knowledge were some issues that we faced. Although there are still more issues to be solved in order to commercialize the currently implemented marketplace, it was verified that various data can be traded after implementing multi-layered security functions in M-Sec marketplace.

Regarding sustainability on future deployment of UC5, please refer to D5.8 for more information.





3 Common Data Governance and Data Protection Policies

M-Sec proposes a set of functional groups in order to enable trust and security in large scale infrastructure such as smart cities. One of the challenges identified by M-Sec project is the management of data subject to regulation, in particular personal data which is protected in Japan by APPI and in Europe by GDPR. We discuss in this section how the different functional groups comply with these regulations given three level of data which are anonymous data, identified data and personal data. This section considers abstract levels of privacy which must be refined per use case, either existing or future according to the regulation. Indeed, while M-Sec provides common data governance for these classes of data, it remains the responsibility of each Use Case to identify which class of data shall be used with a DPIA if required.

3.1 Privacy functions across Functional Groups

The below table from the GDPR report recalls the privacy obligations which are bound to each one of the three classes of data.

Table 3–1. GDPR obligations

GDPR obligation	Identified Data	Pseudonymous Data	Anonymous Data
Notifying data subject about collecting data	Required	Required	Not required
Obtaining consent	Required	Required	Not required
Ability to exercise the right to erasure	Required	Not required	Not required
Ability to exercise the right to access	Required	Not required	Not required
Ability to exercise the right to data portability	Required	Required	Not required
Ability to exercise the right to data rectification	Required	Not required	Not required
Ability to exercise the right to object	Required	Not required	Not required
Presenting basis for cross-border transfer	Required	Required	Not required
Protection by design	Not met	Partially met	Partially met
Data breach notification	Required	Depends on the method	Not required
Data retention limitation	Required	Required	Not required





GDPR obligation	Identified Data	Pseudonymous Data	Anonymous Data
Documentation obligation	Required	Required	Not required
Signing a data processing agreement with a vendor	Required	Required	Not required
Applying the data minimization principle	Advisable	Advisable	Advisable

From these obligations, the following are handled by the M-Sec platform. The others must be handled at use case level.

Ability to access, erase, rectify, object and transfer data

The Security & Storage Functional Group API gathers all endpoints from the Crypto Companion Database and the blockchain. This API is secured by the Security Manager, providing a layer of authentication, so before using any endpoint a set of credentials has to be provided to the user of the API.

This API provides methods to be compliant with the GDPR:

1. Access with the 'read' and 'readAll' endpoints.
2. Erase with the 'delete' and 'deleteAll' endpoints.
3. Rectify with the combination of 'delete' and 'save' endpoints.
4. Transfer with the 'readAll' endpoint.

Presenting basis for cross-border transfer

The access to the IoT Marketplace, where data from different use cases and users could be found and exchanged, is accessible to End-Users through the Web UI and Mobile devices. Additionally, the users of Smile City Report Application are able to connect to the IoT Marketplace. Following the guidelines and requirements from different use cases, such as not storing personal data etc., imposed by GDPR and APPI, the rights are preserved to the destination countries. There was an effort to reduce complexity for End-Users, reduce direct interaction with the Blockchain, and allow them to interact through the Web UI and the Application, as described, and have access to the other components of the overall M-Sec Architecture components and UCs results.

Protection by design

Protection by design is in the DNA of M-Sec, regarding both privacy and cyber-threats. The methodologies, requirement analyses and threat analyses served to make sure data and processes build upon M-Sec components are protected and secure. The different assets of M-Sec, behind the Functional Groups described and implemented in WP3 and WP4 covers altogether the NIST cybersecurity framework as described in next figure:



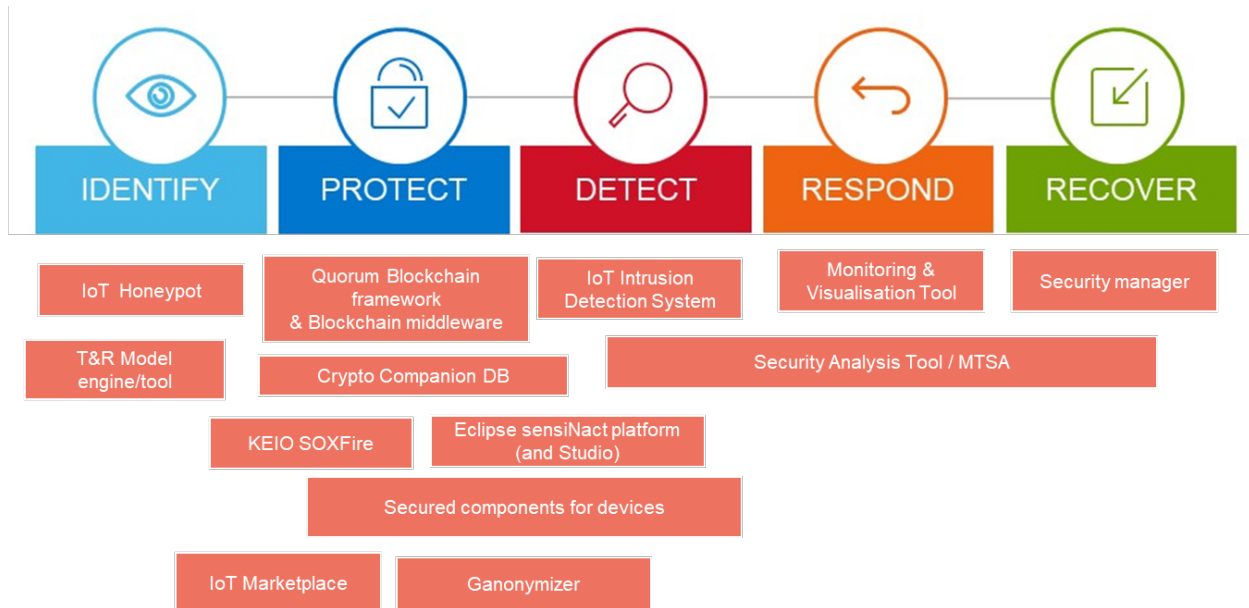


Figure 3—1: NIST cybersecurity framework with M-Sec component mapped to each step

Data breach notification

Users must be notified when a breach of personal data has occurred. Thus, in practice, there is no delay regarding when this notification shall be made, and breach must be actively monitored. This can be proved difficult in case of complex and sophisticated attacks. In addition, when a breach occurred and is detected, it may be hard to identify exactly which data is concerned and one must notify all its user, resulting in reputation harm.

M-Sec provides all the basis to enable automatic breach notification, as described in deliverable 4.10. M-Sec enabled devices are monitored in various ways (IDS, integrity monitoring) and are audited by the security manager. In case of breach, devices can be excluded or put in quarantine while all users registered and attached to these device data are identified by the security manager and then notified of the breach.

Data retention limitation

It is important to note that personal data are not stored in the IoT Marketplace. For sensor data or user generated content such as photos etc. we use an on-chain/off-chain mode. In this direction, we use IPFS or traditional databases to store data, while committing blockchain transactions with the hashed data. This way it is feasible to erase data, in case data needs to be deleted, since it is impossible to retrieve the actual data from the hashed values, while at the same time the hashed content could be used to verify data correctness.

In terms of the Crypto Companion DataBase, on UC2 when a user asks for his/her right to be forbidden, the front-end application has a function to delete all data. Automatically, data from the platform is deleted and a security backup copy is created and stored in case is needed for any regulatory or legal requirements. The copy is stored in a secured way with access restriction methods and access log to keep all the access traceability.





Despite the apparent strictness of the GDPR's data retention periods, there are no rules on storage limitation. For the purposes of the pilot, data is deleted manually after three months once the project has finalized (included in the contractual agreement between WLI and SAN MUN).

3.2 Privacy-cautions for user interfaces applicability per UC

Use Case 1: Secured IoT devices to enrich strolls across smart city parks

In UC1 the Crypto Companion Database (CCDB) is used to encrypt the data and to manage access to data through authentication. Consequently, data can only be accessed by owners and authorised operators (allowed by the owner). At the same time, a hash is generated from all the encrypted data and stored in the Quorum blockchain for data tamper proof.

Fundamental principles are summarised in the following table.

Table 3-2: Use Case1 Fundamental principles

How are the data subjects informed on the processing?	<p>Through the multi-layer information approach, the user is informed. During the registration phase of the website, the user accesses to the first layer, which contains the basic information in a summarised form, at the same time and by the same means as the personal data are collected. Then, additional information is accessible through a link included in the informed consent. (See Figure 2—8: Pilot1 website registration phase: Informed consent).</p>
How can data subjects exercise their rights of access and to data portability?	<p>Within the informed consent, the user has all the information to request his/her right. The controller will respond to the request the latest within one month. The exercise of these rights can be done either through the Santander's website https://sede.santander.es/busqueda-tramites?busqueda=arco. Besides, an email address is available to provide support on this and other matters.</p>
How can data subjects exercise their rights to rectification and erasure?	<p>Within the informed consent, the user has all the information to request his/her right. The controller will respond to the request the latest within one month. The exercise of these rights can be done either through the Santander's website https://sede.santander.es/busqueda-tramites?busqueda=arco. Besides, an email address is available to provide support on this and other matters.</p>
How can data subjects exercise their rights to restriction and to object?	<p>Within the informed consent, the user has all the information to request his/her right. The controller will respond to the request the latest within one month. The exercise of these rights can be done either through the Santander's website https://sede.santander.es/busqueda-tramites?busqueda=arco.</p> <p>A secure copy is created and stored in an encrypted database to be kept for regulation purposes. This is the Trusted and Secure Storage FG. (See Figure 2—9: Architecture of Use Case 1).</p>





In the case of data transfer outside the European Union, are the data adequately protected?

No personal data transfer outside the EU

UC2: Home Monitoring Security System for ageing people

In UC2, FG Secured & Trusted Storage is used to provide rights of access, portability, restriction and erasure. This FG includes methods to access and read data, delete and transfer data. All these methods are implemented in the front-end application of Senior Care so teleoperators can exercise the rights based on end-user's requirements. It is worth to mention that user requests to exercise their rights are received in the contacts established by the telecare company, Atenzia (email and telephone mainly).

Regarding fundamental principles (Controls to protect the personal rights of data subjects)

Table 3-3: Use Case2 Fundamental principles

How are the data subjects informed on the processing?

Atenzia through a visit to end user's home has provided an inform consent to be signed by participants where it is explained Information about the project, the expected duration of the subject's participation, a statement that participation is voluntary, Information about right of Withdrawal or Refusal, right to Rectification, right to Access and of Data Portability, right to Erasure,...

How can data subjects exercise their rights of access and to data portability?

- Right of access: Via common interface (Senior Care Web Responsive). For that is needed an email in order to create the login.
- Right of data portability: Possibility of retrieving, in an easily reusable format by communicating the request to the controller in charge. FG Trusted and Secure Storage that implements methods to access, read, export, delete...

It has been created within the Senior Care Platform a feature to export all data collected from the end user (See **Figure 2—24: Senior Care Exports User's Data**).

How can data subjects exercise their rights to rectification and erasure?

- Within the informed consent, the user has all the information to request his/her right. The controller will respond to the request the latest within one month. The exercise of these rights can be done either through the Santander's website <https://sede.santander.es/busqueda-tramites?busqueda=arco>, or through the various municipal services contacts email and phone number. In addition, Senior Care allows to proceed to the automatic deletion of the user's data from the platform. A secure copy is created and stored in an encrypted database to be kept for regulation purposes. FG Trusted and Secure Storage. (See **Figure 2—25: Senior Care Deletes User Action**)





How can data subjects exercise their rights to restriction and to object?

- Within the informed consent, the user has all the information to request his/her right. The controller will respond to the request the latest within one month. The exercise of these rights can be done either through the Santander's website <https://sede.santander.es/busqueda-tramites?busqueda=arco> , or through the various municipal services contacts email and phone number.

In the case of data transfer outside the European Union, are the data adequately protected?

- No personal data transfer outside the EU

Use case 3: Secure and Trustworthy Mobile Sensing Platform

Components to comply with Privacy strategy on APPI

APPI is not applied because personal information is not handled.

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

Components to comply with Privacy strategy on GDPR & APPI

Regarding fundamental principles (Controls to protect the personal rights of data subjects)

Table 3-4: Use Case4 Fundamental principles

How are the data subjects informed on the processing?	Through the multi-layer information approach, the user is informed. During the registration phase of the website, the user accesses to the first layer, which contains the basic information in a summarised form, at the same time and by the same means as the personal data are collected. Then, additional information is accessible through a link included in the informed consent. (See Figure 2—55: Informed consent for EU citizens (English version) and Figure 2—57: Spanish version of the Informed Consent to be accepted before registration phase).
How can data subjects exercise their rights of access and to data portability?	Within the informed consent, the user has all the information to request his/her right. The controller will respond to the request the latest within one month. The exercise of these rights can be done either through the Santander's website https://sede.santander.es/busqueda-tramites?busqueda=arco .
How can data subjects exercise their rights to	<ul style="list-style-type: none"> • Within the informed consent, the user has all the information to request his/her right. The controller will respond to the request the latest within one month. The exercise of these rights can be done either through the Santander's website https://sede.santander.es/busqueda-tramites?busqueda=arco.





rectification and erasure?

How can data subjects exercise their rights to restriction and to object?

Within the informed consent, the user has all the information to request his/her right. The controller will respond to the request the latest within one month. The exercise of these rights can be done either through the Santander's website <https://sede.santander.es/busqueda-tramites?busqueda=arco>.

From the implementation view point, UC4's smartphone application "SmileCityReport" is considered to have a risk that corresponds to privacy information such as passers-by, especially image rights, in the photos taken by the user, like the general smartphone application of SNS that uses photos.

In the case of image rights not only in SmileCityReport but also in general SNS application, photography beyond the general common-sense limits should be avoided at the user's responsibility, which is within the scope of Informed Consent. Even at a level that does not exceed the general common-sense limit, SmileCityReport addresses the above risks by incorporating a technology that automatically erases privacy information such as people, especially images related to image rights.

In the case of data transfer outside the European Union, are the data adequately protected?

- No personal data transfer outside the EU, because privacy data is removed before sending.

Use case 5: Smart City Data Marketplace with secure Multi-layer Technologies

Components to comply with Privacy strategy on GDPR&APPI

In UC5 the IoT Marketplace and Quorum Blockchain & Blockchain Middleware services are used to enhance security and as a means to anonymize user activity. Additionally, through the integrations between the different assets and Functional Groups such as the integration among IoT Marketplace FG and End to End FG, the anonymization and compliance with GDPR and APPI are ensured. To this direction, users are able to interact with the different services with no personal data stored in the IoT Marketplace.

GDPR is not applied because personal information is not handled.





4 Conclusions

This document provides a final report of the five M-Sec pilots carried out in both cities, Fujisawa and Santander, during the third year of the project.

This report includes detailed information on the scenario and set up of each one of the M-Sec pilots, describing its reorientation due to the pandemic situation as occurred in UC4; the identification of the main challenges due to the COVID-19 together with mitigation actions to address the identified challenges, which have helped to minimize their impact on pilots' setup, on the engagement process with citizens and stakeholders, as well as on the level of participation in the different pilots. In order to evaluate each of the pilots, a series of KPIs have been defined and a questionnaire has been distributed among the participants, both included in this deliverable and which main results can be found in deliverable D2.8. From the technical approach, an updated version of the architecture is also included, highlighting the security introduced by the components developed within the M-Sec project. In terms of privacy in the pilots, the data protection policies and processes applied are also described, showing how the implementation of the pilots complies with the GDPR/APPI, as well as which M-Sec components are used to ensure this compliance.

Finally, the pilot report follows an iterative approach, whereby the current deliverable is the third report on the M-sec pilots, which completes and updates the information provided in previous deliverables, D2.3.1 and D2.3.2.





Annex 1 – UC4 representative agreement

Click on the following figure to access the Representative Agreement signed by Keio University and Santander city council.

GDPR ARTICLE 27 REPRESENTATIVE AGREEMENT

This GDPR Article 27 Representative Agreement (this “Agreement”) is entered into by and between Keio University, with offices located at 5322 Endo, Fujisawa-shi, Kanagawa 252-0882 Japan (the “University”), and Santander City Council, with offices located at Plaza Ayuntamiento, 1, 39002 Santander, Cantabria, Spain (the “Designee”, and together with the University, the “Parties”, and each a “Party”) only in the framework of the M-Sec project.

RECITALS

WHEREAS, the University and the Designee are in a consortium of M-Sec Project funded by European Commission (EC) and National Institute of Information and Communications Technology (NICT);

WHEREAS, the University Processes certain Personal Data of Data Subjects in the European Union (the “EU”), as provided in [Appendix 1](#) attached hereto and incorporated into this Agreement by reference;

WHEREAS, the Designee is established in Spain, which is one of the Member States of the EU where Data Subjects, whose Personal Data the University Processes are, or will be located; and

WHEREAS, the University desires to designate the Designee as a Representative of the University in the European Union to act on its behalf with regard to its obligations under Article 27 of the GDPR in the framework of the M-Sec project and the Designee is willing to accept such designation in accordance with the terms and conditions set forth herein;

NOW, THEREFORE, in consideration of the mutual covenants and agreements set forth herein, the Parties hereby agree as follows:

1. **Definitions.** Capitalized words and phrases not defined herein shall have the same definitions as in the General Data Protection Regulation (2016/679) of the European Parliament and of the Council (the “GDPR”). Capitalized words, terms, or phrases that are not defined herein or in the GDPR shall be considered typographic errors, unless context or custom dictates otherwise.
2. **Designation as Representative.**
 - 2.1. The University hereby designates the Designee, and the Designee hereby accepts such designation, as the Representative for the University pursuant to Article 27 of the GDPR within the framework of the M-Sec project.



GDPR ARTICLE 27 REPRESENTATIVE AGREEMENT

This GDPR Article 27 Representative Agreement (this “**Agreement**”) is entered into by and between Keio University, with offices located at 5322 Endo, Fujisawa-shi, Kanagawa 252-0882 Japan (the “**University**”), and Santander City Council, with offices located at Plaza Ayuntamiento, 1, 39002 Santander, Cantabria, Spain (the “**Designee**”, and together with the University, the “**Parties**”, and each a “**Party**”) only in the framework of the M-Sec project.

RECITALS

WHEREAS, the University and the Designee are in a consortium of M-Sec Project funded by European Commission (EC) and National Institute of Information and Communications Technology (NICT);

WHEREAS, the University Processes certain Personal Data of Data Subjects in the European Union (the “**EU**”), as provided in Appendix 1 attached hereto and incorporated into this Agreement by reference;

WHEREAS, the Designee is established in Spain, which is one of the Member States of the EU where Data Subjects, whose Personal Data the University Processes are, or will be located; and

WHEREAS, the University desires to designate the Designee as a Representative of the University in the European Union to act on its behalf with regard to its obligations under Article 27 of the GDPR in the framework of the M-Sec project and the Designee is willing to accept such designation in accordance with the terms and conditions set forth herein;

NOW, THEREFORE, in consideration of the mutual covenants and agreements set forth herein, the Parties hereby agree as follows:

1. Definitions. Capitalized words and phrases not defined herein shall have the same definitions as in the General Data Protection Regulation (2016/679) of the European Parliament and of the Council (the “**GDPR**”). Capitalized words, terms, or phrases that are not defined herein or in the GDPR shall be considered typographic errors, unless context or custom dictates otherwise.

2. Designation as Representative.

2.1. The University hereby designates the Designee, and the Designee hereby accepts such designation, as the Representative for the University pursuant to Article 27 of the GDPR within the framework of the M-Sec project.

- 2.2. The Designee agrees to be addressed, in addition to or instead of the University, by Supervisory Authorities and Data Subjects, on all issues related to Processing by the University, for the purposes of ensuring the University's compliance with the GDPR within the framework of the M-Sec project.

3. Responsibilities of the Designee. The Designee shall:

- 3.1. Receive, relay, and, after consultation with the University, respond as directed by the University to any communications from Supervisory Authorities or Data Subjects on all issues related to the Processing of Personal Data by the University.
- 3.2. Immediately notify the University using the most efficient method of notice available to it if it receives any communications from Data Subjects or Supervisory Authorities, as described in Section 3.1. In any case, such notification shall be provided to the University no later than seventy-two (72) hours from the moment the communication is received by the Designee.
- 3.3. Fully and promptly cooperate with Supervisory Authorities, on the University's behalf, as directed by the University, as necessary to enable the University to comply with its obligations under the GDPR.
- 3.4. Make the Record available to Supervisory Authorities at their request.
- 3.5. Keep the contact details required for cooperation with the Data Subjects and Supervisory Authorities (the "**Public Contact Information**"), accurate and up-to-date at all times. Should the contact details change, the Designee will notify the University without undue delay.
- 3.6. Appoint a natural person who will communicate with the Data Subjects and Supervisory Authorities in the official language of the country in which the Designee is established.

4. Designee's Public Contact Information. The Designee's Public Contact Information in the EU shall be as follows:

[COMPANY NAME]: Santander city council

[ADDRESS]: Plaza Ayuntamiento, 1, 39002 Santander, Cantabria, Spain

[EMAIL ADDRESS]: protecciondedatos@santander.es

[NAME OF THE NATURAL PERSON AND POSITION TO ACT IN ACCORDANCE WITH SECTION 3.6. ABOVE]: Mr. Rosendo Ruiz Pérez, Chief of the Technical Office for Safety and Security and DPO.

5. Obligations of the University. The University shall:

- 5.1. Provide all the information required under Section 5.1 to the Designee on or before the Effective Date of this Agreement and keep such information accurate and up-to-date at all times.
- 5.2. At all times, provide all the information necessary for the Designee to fulfill its obligations as provided under this Agreement.
- 5.3. Maintain a record of Processing activities as required pursuant to Article 30(1) or Article 30(2), as applicable (the “**Record**”). The Record shall contain all of the following information:
 - (a) the name and contact details of the University, in its role as Controller, and, if applicable, the Joint Controller and the Controller’s Data Protection Officer;
 - (b) the purposes of the Processing;
 - (c) a description of the categories of Data Subjects and of the categories of Personal Data;
 - (d) the categories of recipients to whom the Personal Data have been or will be disclosed, including recipients in Third Countries or International Organisations;
 - (e) transfers of Personal Data to a Third Country or an International Organisation, including the identification of that Third Country or International Organisation and, in the case of transfers referred to in the second subparagraph of Article 49(1) of the GDPR, the documentation of suitable safeguards;
 - (f) where possible, the envisaged time limits for erasure of the different categories of data; and
 - (g) where possible, a general description of the technical and organisational security measures referred to in Article 32(1) of the GDPR.

6. Notices. All notices, demands, or requests given by the Parties shall be transmitted by e-mail to the address that the Parties have designated in this Section 7:

6.1. To the University at jn-msec@sfc.keio.ac.jp.

6.2. To the Designee at protecciondedatos@santander.es.

7. Term and Termination.

7.1. The term of this Agreement shall take effect on [May 14, 2021] (the “**Effective Date**”) and shall continue until [September 30, 2021] (the “**Term**”).

8. Representations and Warranties; Disclaimer.

8.1. Each Party represents and warrants to the other Party that:

- (a) it has all right, title, and authority to enter into this Agreement;
- (b) its execution of this Agreement and its performance of its obligations hereunder do not constitute a breach of any contract, agreement, or understanding, oral or written, to which it is a Party or by which it is bound; and
- (c) it is not the subject of an allegation, of which it has been notified by any known authority in any country, including without limitation the Attorney General of any state or province, the United States Federal Trade Commission, any law enforcement agency or any foreign data protection authority, concerning the misuse of personal data.

8.2. The Designee further represents, warrants, and covenants to the University that:

- (a) the Designee is legally established in Santander, Spain; and
- (b) the Designee shall perform the responsibilities described in Section 3, in accordance with the terms of this Agreement, and applicable law, including but not limited to the GDPR and the laws of the EU Member State in which the Designee is established.

8.3. The University further represents, warrants, and covenants to the Designee that it has all necessary right, title, and authority to designate the Designee as its Representative and to bestow upon it the mandates of this Agreement.

9. Indemnification.

9.1. Each Party agrees to defend, indemnify, and hold the other Party and its officers, directors, employees, agents, subsidiaries, and affiliates harmless from and against any and all claims, losses, liabilities, damages, judgments, awards, expenses, actions, lawsuits, and costs, including, without limitation, reasonable attorneys' fees, directly arising out of or relating to third-party claims based on either Party's actual:

- (a) grossly negligent acts or omissions, or fraud in connection with this Agreement; infringement of a third party's intellectual property rights; or

- (b) violation of any statute, law, ordinance, or regulation, resulting from the University's failure to comply with this Agreement; and
- (c) provided in each case that each Party complies with the indemnification procedures of Section 10.2 below.

The Parties agree that "gross negligence" is defined as conduct that is indicative of intentional wrongdoing or evinces a reckless indifference to the rights of others.

9.2. Indemnification Procedures. With respect to a Party's obligation to indemnify (the "**Indemnifying Party**") the other Party (the "**Indemnified Party**") shall:

- (a) provide the Indemnifying Party with prompt written notice of any such claim, action, or demand for which indemnity is sought;
- (b) allow the Indemnifying Party to control the defense and related settlement negotiations, provided, however, that the Indemnified Party shall have the right to participate in such defense with counsel of its own choosing at its own expense;
- (c) provide the Indemnifying Party, at the Indemnifying Party's request, with reasonable assistance in the defense of such claim, action or demand, so long as the Indemnifying Party reimburses the Indemnified Party for the Indemnified Party's reasonable out-of-pocket expenses associated therewith; and
- (d) not settle a claim without the Indemnified Party's written consent, which consent shall not unreasonably be withheld. The Indemnifying Party shall not be relieved of its indemnification obligations herein for the Indemnified Party's failure to comply with such requirements, except to the extent that the Indemnifying Party has been prejudiced by the Indemnified Party's actions or inactions.

10. Receipt of Confidential Information.

10.1. Definition. In the course of performing duties under this Agreement, the Designee may obtain Confidential Information (as defined below) from the University. "**Confidential Information**" means any and all technical and non-technical proprietary information provided by the University to the Designee, whether disclosed orally or in writing, Personal Data, and includes all other information regarding:

- (a) the terms of this Agreement; and

- (b) any information which is marked or designated as confidential or proprietary at or prior to disclosure or which would appear to a reasonably prudent person to be confidential and/or proprietary in nature.

Confidential Information does not include information or data that the Designee can show by credible evidence:

- (a) was in the public domain at the time it was communicated to the Designee;
- (b) entered the public domain subsequent to the time it was communicated to the Designee through no fault of the Designee;
- (c) was in the Designee's possession, not in violation of any obligation of confidentiality, at the time it was communicated to the Designee;
- (d) was disclosed to the Designee not in any violation of any obligation of confidentiality; or
- (e) was independently developed by the Designee without use of or reference to the Confidential Information of the University.

10.2. Restrictions on Use and Disclosure. The Designee agrees to hold the Confidential Information of the University in confidence, using the same degree (but no less than a reasonable degree) of care and protection that it uses to protect its own proprietary information, both during and after the Term of this Agreement. The Designee agrees not to use or disclose the Confidential Information for any purpose other than as necessary to fulfill its obligations or exercise its rights under this Agreement and agrees to take all reasonable steps to ensure that Confidential Information is not used, disclosed, or distributed by its employees or agents in violation of the terms of this Agreement. Notwithstanding anything contained herein to the contrary, the Designee may disclose Confidential Information pursuant to an order of a court of competent jurisdiction or as otherwise required by applicable law. Under such circumstances the Designee will, if reasonably possible under the circumstances, provide the University with advance notice of such disclosure in order to afford the University an opportunity to take legal action to prevent or limit the scope of such disclosure, and will cooperate with the University in connection therewith.

10.3. Return or Destruction of Confidential Information. Upon termination of this Agreement or otherwise at the University's written request the Designee shall, at the University's option, either return to the University or destroy all Confidential Information (including all copies thereof) in the Designee's possession, custody and control.

11. Miscellaneous.

- 11.1. Governing Law; Jurisdiction; Venue; Attorneys' Fees.** This Agreement shall be governed by and construed in accordance with the laws of Belgium. Any dispute, controversy or claim arising under, out of or relating to this agreement between the University and the Designee which cannot be resolved by mutual agreement and any subsequent amendments of this contract, including, without limitation, its formation, validity, binding effect, interpretation, performance, breach or termination, as well as non-contractual claims, shall be submitted to mediation in accordance with the WIPO Mediation Rules. The place of mediation shall be Tokyo, if the Designee requests the mediation, or Brussels, if the University requests the mediation, unless otherwise agreed upon. The language to be used in the mediation shall be English unless otherwise agreed upon. Both the University and the Designee waive any objection based on *forum non conveniens* or any objection to venue of any such action. In any action to interpret or enforce this Agreement, the prevailing Party shall be entitled to seek an award of all court costs and reasonable attorneys' fees it incurs.
- 11.2. Force Majeure.** No Party shall be liable or responsible to the other Party, nor be deemed to have defaulted under or breached this Agreement, for any failure or delay in fulfilling or performing any term of this Agreement, when and to the extent such failure or delay is caused by or results from acts beyond the affected party's reasonable control ("**Force Majeure Event**"), including, without limitation: (a) acts of God; (b) flood, fire, earthquake, or explosion; (c) war, invasion, hostilities (whether war is declared or not), terrorist threats or acts, riot, or other civil unrest; (d) government order or law, including the invalidation of any applicable regulation or data protection framework or mechanism; (e) actions, embargoes, or blockades in effect on or after the date of this Agreement; (f) action by any governmental authority; (g) national or regional emergency; (h) strikes, labor stoppages or slowdowns, or other industrial disturbances; and (i) shortage of adequate power or transportation facilities. The Party suffering a Force Majeure Event shall give notice as soon as reasonably possible to the other Party, stating the period of time the occurrence is expected to continue and shall use diligent efforts to end the failure or delay and ensure the effects of such Force Majeure Event are minimized.
- 11.3. No Waiver.** Any waiver or the failure of either Party to this Agreement to object to or take affirmative action with respect to any conduct of the other which is in violation of the terms of this Agreement shall not be construed as a waiver of the violation breach, or of any future violation, breach or wrongful conduct.
- 11.4. Severability.** It is intended by the Parties that all provisions of this Agreement be severable. If any term or provision hereof is illegal or invalid for any reason whatsoever, such illegality or invalidity shall not affect the validity or legality of the remainder of this Agreement, and any such unenforceable term or provision shall

be modified to the minimum extent necessary to make the term or provision enforceable.

- 11.5. Amendment.** Notwithstanding any provisions in any other agreement between the Parties regarding modifications or amendments, no modification of or amendment to this Agreement, nor any waiver of any rights under this Agreement, will be binding upon either Party, unless made in writing and signed by a duly authorized representative of each Party.
- 11.6. Survival.** Sections 7, 8, 9, 10, 11, 12, 13.4 and this “Survival” provision and any other provisions that by their nature ought to survive this Agreement shall survive termination of this Agreement regardless of the manner in which this Agreement was terminated.
- 11.7. Assignment by the University.** The University may assign its rights and obligations under this Agreement if the proposed assignee assumes all the obligations of the University under this Agreement and the Designee is notified in writing thirty (30) days prior to such assignment.
- 11.8. Assignment by the Designee.** In the case of a change of control of the Designee, the Designee may assign its rights and obligations under this Agreement to the entity that assumes control of the Designee, provided that: (a) the University is notified in writing at least thirty (30) days prior to such assignment; and (b) the University shall have a right to reasonably object to the proposed assignment. All other proposed assignments shall require the written consent of the University.
- 11.9. Successors and Assigns.** This Agreement shall be binding upon and shall inure to the benefit of the Parties hereto and their respective successors and permitted assigns.
- 11.10. Entire Agreement; Waiver; No Third-Party Beneficiaries.** This Agreement and the appendices hereto constitute the entire agreement between the Parties as to the subject matter hereof, and supersede all prior and contemporaneous agreements, representations and understandings between them relating thereto, except as may be expressly incorporated by reference into this Agreement. No waiver of any provision of this Agreement shall be deemed, or shall constitute, a waiver of any other provision, nor shall any waiver constitute a continuing waiver. No waiver shall be binding unless executed in writing by the Parties. Except as expressly provided for herein, this Agreement is not for the benefit of any third party.
- 11.11. Counterparts.** This Agreement may be executed in counterparts, each of which shall be deemed an original, but all of which together shall be deemed to be one and the same agreement. A signed copy of this Agreement delivered by facsimile,

email, or other means of electronic transmission shall be deemed to have the same legal effect as delivery of an original signed copy of this Agreement.

IN WITNESS WHEREOF, the Parties have hereunto set their hands as of the dates indicate below.

UNIVERSITY

DESIGNEE

Signature



Signature



Name

JIN NAKAZAWA

Name

Rosendo Ruiz

Title

Professor

Title

Chief of the Technical Office for Safety and Security and DPO

Company Name

Keio University

Company Name

Santander City Council

Date

May 14, 2021

Date

May 13, 2021

Appendix 1

Details Regarding Processing of Personal Data of Data Subjects in the European Union

[PROVIDE DETAILS OF DATA PROCESSING TO OCCUR]

Categories of Personal Data

The categories of personal data are: IP address of the smartphone, location information of the smartphone, photos taken by field trial participant (surrounding landscape), photos taken by field trial participant (face and mainly the upper body), smile degree of field trial participant estimated from the photo (face and mainly the upper body), and the smartphone sensor information, age, gender, occupation, address (country / prefecture unit), survey results, email address.

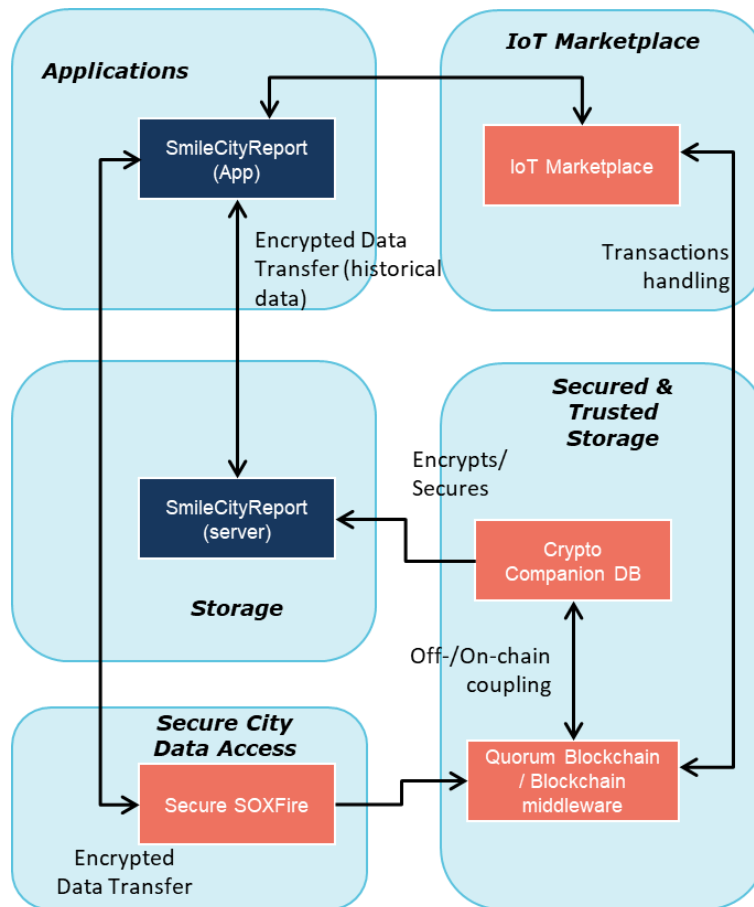
Purposes of the Processing

The purposes of the processing are: The location information and posted information of field trial participants are collected as reports on local events using the participants' smartphones. Assuming that the collected data will be bought and sold in the marketplace, we will verify that it can be distributed and traded securely and globally.

Detailed description of data processing as below:

- A user downloads and installs the SmileCityReport app on his/her mobile phone.
- The informed consent shall be accepted by the user before running the app.
- Registration process: user shall provide the following information:
 - o data requested: nickname, password, gender, range of age, occupation, zip code.
- Join a theme (or several themes) and start posting pictures and comments.
 - o A user may post a picture using both cameras, and add comments.
- Regarding data collected during registration process as well as post process, input data is stored in SmileCityReport server and huddled securely by Secure SOXFire within Keio mobile sensing platform. And when these data is handled in marketplace, these data is sent securely via Crypt Companion DB and Quorum Blockchain to IoT marketplace.
- The personal information like IP address of the smartphone and the email address are handled by secure manner as well as posted data described in previous section.
- The personal data leak is avoided by handling these data by multi-layer security solutions supported by M-Sec.

- The posted data and some personal data which is needed for exchanging data and its consideration. These minimum data goes to the Marketplace in secure manner.



Categories of Data Subjects

The categories of data subjects are: Field Trial Participants, including at least SmileCityReport app end-users as well as Marketplace users.

Recipients of the Personal Data

The recipients of the personal data are: Keio University and NTTE.

Types of Sensitive Data (if any)

The types of sensitive data processed are: [_No sensitive data].