Multi-layered Security Technologies

for hyper-connected smart cities

D2.3.2: M-Sec pilots definition, setup and citizen involvement report – First version

November 2020

Grant Agreement No. 814917

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

Project acronym	M-Sec
Deliverable	D2.3.2 M-Sec pilots definition, setup and citizen involvement report – 1st version
Work Package	WP2
Submission date	November 2020
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	26Oct2020	Keiko Doguchi(NTTE)	ToC
v0.2	9Nov2020	Akira Tsuge (Keio)	UC4 description as first draft
v0.3	9Nov2020	Arturo Medela (TST)	UC1 initial contribution
v0.4	9 Nov 2020	Vanessa Clemente (WLI)	UC2 initial contribution
v0.5	11 Nov 2020	George Palaiokrassas (ICCS)	UC5 contribution
v0.6	12 Nov 2020	Akira Tsuge (Keio)	UC3 initial contribution
v0.7	16 Nov 2020	Sonia Sotero (AYTOSAN)	Introduction provided
v0.8	17 Nov 2020	Keiko Doguchi(NTTE)	UC5 and conclusion contribution and some comments
v0.9	19 Nov 2020	George Palaiokrassas (ICCS)	UC5 finalisation
v0.10	23 Nov 2020	Arturo Medela (TST)	UC1 2nd contribution
v0.11	25 Nov 2020	Sonia Sotero (AYTOSAN)	UC4&UC5 contributions
v0.12	25 Nov 2020	Vanessa Clemente (WLI) & Sonia Sotero (AYTOSAN)	UC2 contribution
v0.13	26 Nov 2020	Orfeas Voutyras (ICCS)	Internal review
v0.14	27 Nov 2020	Akira Tsuge (Keio)	UC3 & UC4 contribution
v0.15	27 Nov 2020	Kenji Tei (WU)	Internal review
v0.16	27 Nov 2020	Mari Seki (NTTE)	UC4 contribution
v0.17	27 Nov 2020	Vanessa Clemente (WLI)	Answer to UC2 comments
v0.18	30 Nov 2020	Keiko Doguchi (NTTE)	UC5 contribution
v0.19	30 Nov 2020	Keiko Doguchi (NTTE)	Answer to UC 5 comments, added mitigation chart of all UCs
v0.20	30 Nov 2020	Akira Tsuge (Keio)	UC4 contribution
v0.21	30 Nov 2020	George Palaiokrassas (ICCS)	Answer to UC 5 comments
v0.22	30 Nov 2020	Arturo Medela (TST)	Answer to UC1 comments
v0.23	30 Nov 2020	Sonia Sotero (AYTOSAN)	Integration of partner contributions
v0.24	30 Nov 2020	Sonia Sotero (AYTOSAN)	UC2 & UC4 surveys as annexes
v0.25	30 Nov 2020	Akira Tsuge (Keio)	Answer to UC3 comments
v0.26	01 Dec 2020	Mari Seki (NTTE)	Replaced architecture view charts for all UCs
v1.0	01 Dec 2020	Keiko Doguchi (NTTE)	Final

Table of Contents

List of Tables

List of Figures

Glossary

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

1 Introduction

1.1 Scope of the document

The main purpose of deliverable 'D2.3 M-Sec pilots definition, setup and citizen involvement report – 1st version' is to provide an assessment of the pilots carried out in both cities, Santander and Fujisawa. However, due to the coronavirus, none of the M-Sec pilots were able to start by June 2020, when this deliverable was scheduled to be submitted.

Consequently, M-Sec consortium agreed to submit two versions of this deliverable: a first version, which was submitted in July 2020, provides a detailed overview of the pilots' initial plan; and a second version which includes the main outcomes, feedback from end-users and stakeholders as well as lessons learnt from the first trial of the pilots. The second version of the D2.3 deliverable is the current document, which also takes into account feedback from the 2nd year project review. We named this deliverable "D2.3.2" so that it is clearly defined as the following version of D2.3.

Finally, the document follows an iterative approach by submitting a new version at the end of the project, Deliverable 2.4, once the results of the second trial of the M-Sec pilots have been assessed.

2 M-Sec Pilots

This section provides results of the pilots that were carried out in Santander and Fujisawa, in order to validate the use cases defined in D2.1 and update the plan described in D2.2. As we already reported and got approved, now we have five use cases and five pilots. Two use cases/pilots are in Santander, one use case/pilot is in Fujisawa and two use cases/pilots are cross border.

Table 1 Updated Use Cases and Pilots

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

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

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

Pilot scenario and objectives

The main idea behind pilot 1 consists of deploying IoT devices that measure variables significant to the wellbeing of the city's inhabitants, such as noise or CO_2 levels, and overcrowding of selected areas through the sketching of heat maps. This information is relevant for the Municipality as well since it is not covered as of today as part of the smart city deployments already existing and this data would help when analysing the area and programming specific actions.

Users interested in taking part in the experience will find QR codes scattered throughout the pilot site (Las Llamas Park in Santander) for them to join the pilot. A web application will enable these users to access and rate the quality of the data submitted, providing another layer of validation. Such activity will be encouraged via a rewards system targeting the most active users on the site.

Figure 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

Given the situation provoked worldwide by the COVID-19 pandemic and to prevent its impact over the execution of the diverse M-Sec use cases, partners in the consortium evaluated the main challenges that may rise and proposed a series of mitigation actions to let the pilots take place adequately and without major deviations and/or risks for any of the parties involved.

First and foremost, there is a more than probable chance that the sanitary conditions impulse national or regional governments to go back to a total lockdown scenario or the implementation of severe restrictions in terms of mobility. In the particular case of Pilot 1, M-Sec will face this challenge by facilitating access through the web app to the different menus and measurements; this way, potential interested users and stakeholders would have means to retrieve information even though they are not able to be present at the Las Llamas Park where the experience takes place.

Another challenge is directly related to the appearance of technical issues in the devices deployed as part of the pilot. The way to solve these situations will imply a process within the consortium to assure a quick reaction to solve potential failures and/or theft of deployed devices. The former will be solved thanks to periodic interaction among partners involved to polish integrations and act over potential issues. Both this and the latter will need the collaboration of Santander Municipality to issue the proper permissions to let partners go to the park and conduct the required actions.

Finally, two additional challenges that are closely related refer to the low interest the pilot in its non-presential version could raise and thus the recruitment of a low number of users. To mitigate this, it is important to get feedback about what could be more attractive to end users and try to apply it and trigger alternative means of recruitment once there is no option to meet in the same physical room; online meetings via different tools will be considered to mitigate this potential challenge and have on board the minimum number of participants to ensure that the results obtained are enough to properly evaluate the M-Sec solution.

Table 2 below summarizes all these challenges and a brief explanation on how they will be addressed.

Table 2: Use Case 1 challenges and mitigations

Challenge	Description	Mitigation Action
1	COVID related 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.

Challenge	Description	Mitigation Action
4	Low number of participants	Trigger alternative means of recruitment, even online ones (meetings via Zoom/Teams?).

Engagement process with citizens and stakeholders

The current pandemic situation and the restrictions applied in Cantabria, the Spanish region where Santander is located, constitute a roadblock in the recruitment and engagement process initially devised and the one later updated accordingly.

This is the reason why the engagement process for the initial stage of Pilot 1 reduced its scope. In the end, the initial users will mainly include Santander Municipality representatives that will check how the measurements offered can be of any help to their daily routines.

In addition, and taking into account the stakeholders envisioned for Pilot 1, as depicted in Figure 2, some citizens were invited to take part in this initial stage. The way to get in touch with them was through direct one-on-one conversations, and they will help partners involved in this use case to improve the pilot.

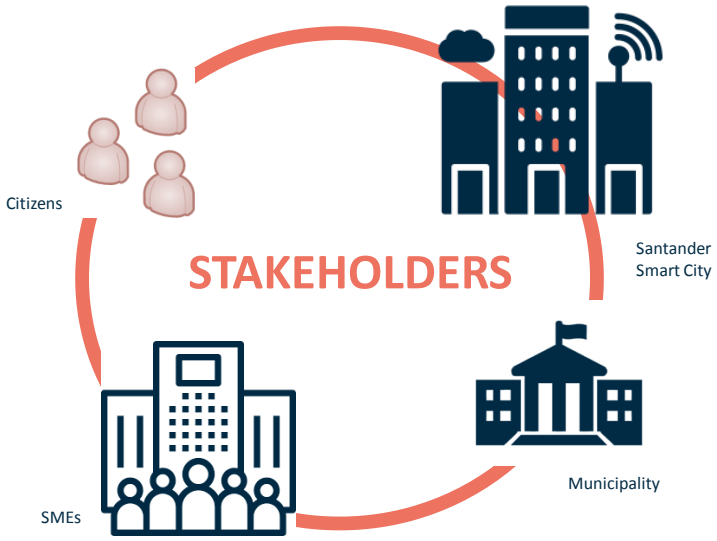


Figure 2: M-Sec Pilot 1 main stakeholders

Moreover, one workshop has taken place just a couple of weeks after the start of the pilot involving representatives of the Environmental Services in the Santander Municipality, and oriented to presenting them the tool and getting their feedback on how it works and how it could improve. Figure 3 below summarizes the main conclusions obtained.

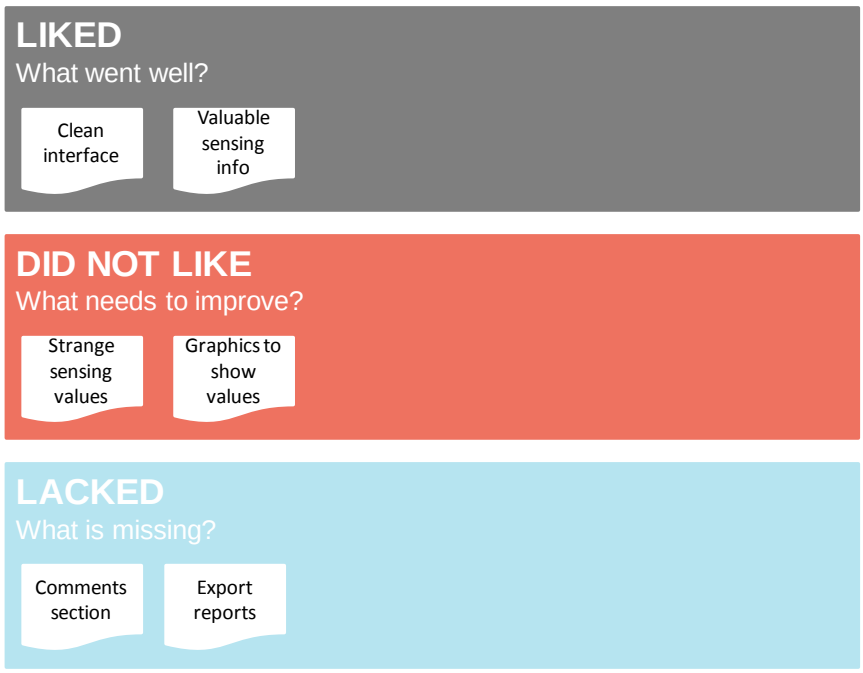


Figure 3: Use Case 1 initial workshop evaluation results

On the positive side, users liked the clean interface provided through the web application, which tries to follow and stick to the style of another websites related to Santander Municipality. In addition, the information provided by the different sensors is considered as valuable, at least during this initial stage,

On the other hand, users did not like to see strange sensing values from time to time, not quite representatives of the city of Santander, neither the way to represent these measurements via tables: the preference to have them painted in graphs is patent.

Last but not least, these initial users mentioned they feel the web application lacks of a comments section and wondered about the potential availability of some method to export sensing reports to files in diverse formats. That is something that will be taken into account in the further iterations of the solution.

On the next iteration, and hoping the sanitary situation improves, the plan is to hold meetings with various people in attendance coming from different contexts and involving academia and SMEs that may be interested in taking part to a system like this.

Technical approach – M-Sec components

Pilot 1 involves the integration of several components in the M-Sec framework as it can be seen in Figure 4 below extracted from WP3, Task 3.2, as extensively explained in Deliverable 3.4.

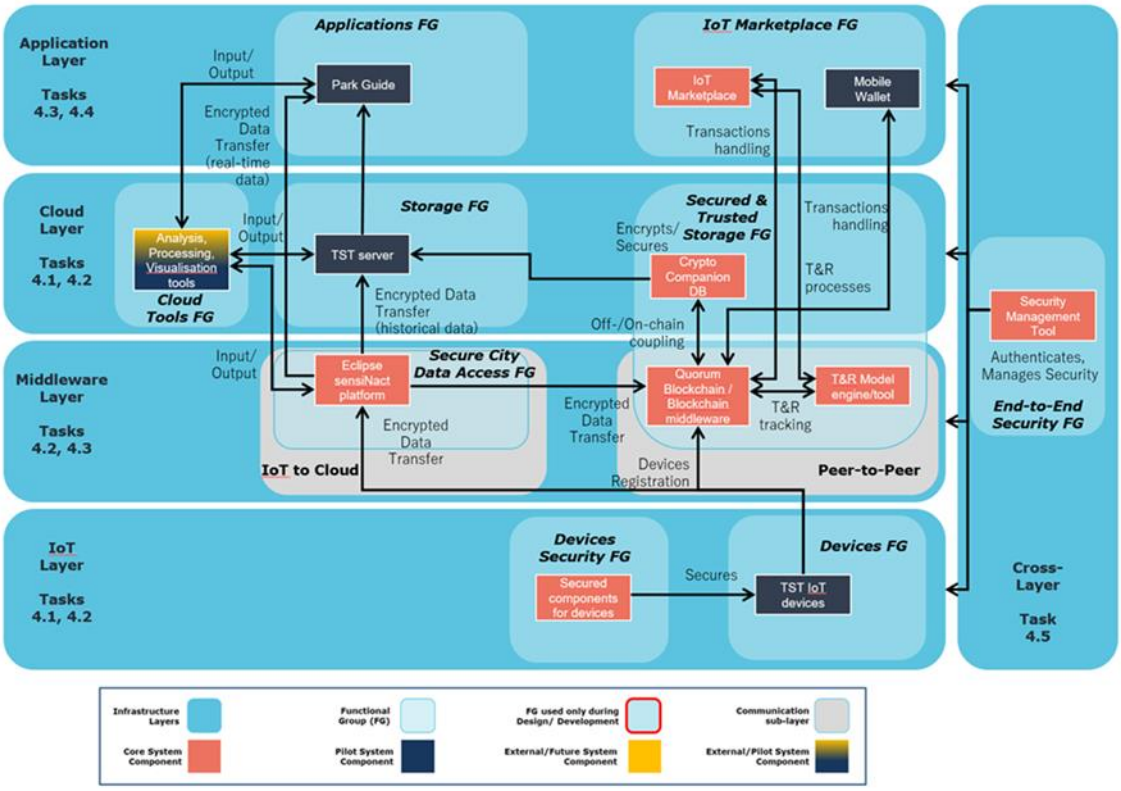


Figure 4: Use Case 1 architectural view

Starting from the lower layer, the system relies in two different IoT devices developed within the project. Some of them are the so called crowd counting devices, which are capable of detecting Wi-Fi and BT MAC addresses and offering a figure which is an estimation of the number of people in attendance in the surroundings of that specific spot at that moment in time. The first of these devices is located (see Figure 5) in one of the hot spots of the Las Llamas Park, just in the level below its restaurant.

Figure 5. Crowd counting device in Pilot 1

The other devices installed are in charge of performing environmental monitoring duties through five different sensors, namely: temperature, humidity, CO_2, VOC and noise. The locations considered imply covering on the one hand the children playground area and on the other hand a complete longitudinal section of the park, going from one side, closer to the University of Cantabria, to the other, just next to a residential area, covering as well the city motorway which separates this housing zone and the park itself. Figure 6 presents three out of the five devices deployed across the park.

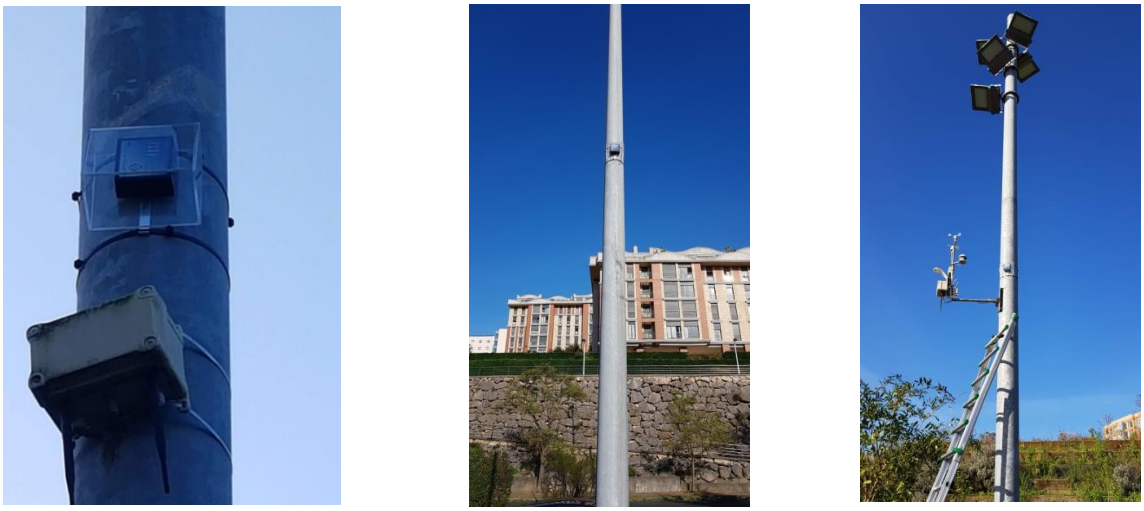


Figure 6: Environmental Monitoring devices in Pilot 1

In the search to complement the service offer, the system offers extended information about nine specific points of the park, some of them coincidental with the sensing devices deployment spots, where visitors receive specific data about what they can find there. To enable M-Sec pilot users to access this data, nine QR codes have been distributed throughout the park (see two examples in Figure 7). Reading these codes allows access to the web application that presents this information together with the data collected by the IoT devices, properly decrypted in the server. In the web app, which is ingrained in the M-Sec application layer, people can join the pilot through a simple registration process and thus have access to all the data offered.

Figure 7. QR Codes to access web application in Pilot 1

Once registered, users may visit the specific sections allocated to those nine places to visit or to the IoT devices scattered though the park, where they will be able to check the information and measurements registered and even deposit their satisfaction degree through a simple 5-star rating method that will help M-Sec partners in charge of Use Case 1 get to know how useful the service is according to its participants. Some screenshots of the web application follow in Figure 8.

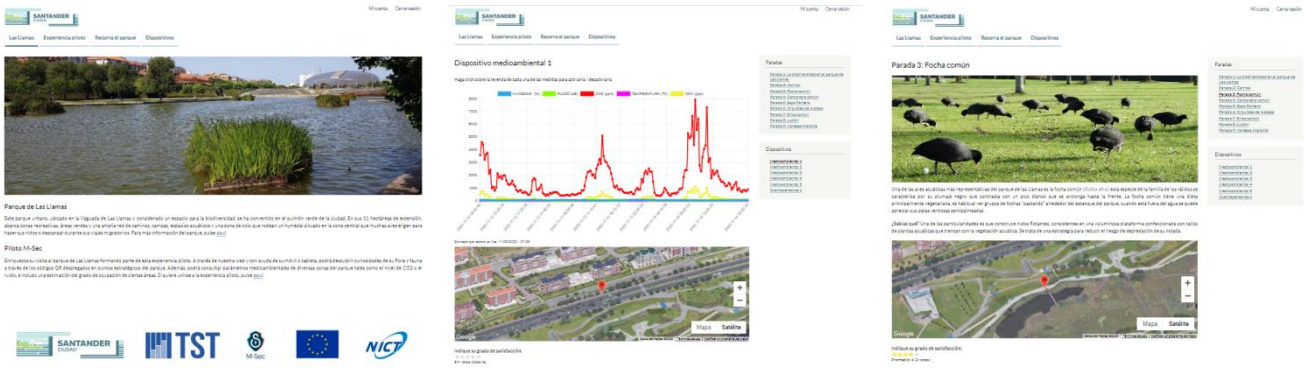


Figure 8: Use Case 1 web application features

The next immediate steps in the Pilot 1 evolution imply sending the data collected by the IoT devices to the Eclipse sensiNact Platform through an MQTT connection. There, sensiNact users will be able to visualize the devices and the data and establish their very own analysis.

Afterwards, once data is collected, it will be sent to the server, proceeding to encrypt sensitive data using the M-Sec tool known as Crypto Companion Database (CCDB), which is a system that encrypts the data with an asymmetric public/private key pair. Data will 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.

Finally, and since all data collected from the sensors integrated in the IoT devices can be publically available because it doesn't contain any personal data related to the end user, it will be transferred to the M-Sec marketplace where stakeholders who may be interested on getting this kind of environmental and occupancy data can buy it using the so-called M-Sec Tokens, which is a cryptocurrency in the form of a smart contract running in on blockchain as discussed in other sections.

KPIs and Evaluation

To achieve success, KPIs were defined in the previous version of the current deliverable submitted in July 2020. As not all of the KPIs have been reached as the trial is still ongoing, we have updated only those metrics that could reflect the current status of the project:

Table 3. Use Case 1 Pilot 1 KPIs

#KPI	Goal	How to measure?	Target	Target Achieved 1st Phase
#Participants	Minimum number of end users to test the solution provided	Number of end users registered into the system	≥50 users (1st trial: 10-15 friend users, 2nd trial: 50 participants)	10
#Active users	To evaluate the real activity of registered participants	Connections to the web app	≥50	6
#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	--
#Unauthorised intents to access to data	Avoid unauthorised users have access to sensitive data	Through smart contracts, it is possible to verify whether someone has authorization or not. Warning logs will be received to alert about it.	0	--
#DDoS attacks	Avoid attempts to disrupt normal traffic	Putting IoT devices on the Internet before going public and evaluating their interactions.	0	0

#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	0

It is worth noting that when dealing with KPIs involving external malicious actors trying to hack the system and anticipating that perhaps not many of them are going to act over this particular pilot deployment, M-Sec partners involved in this pilot will conduct tests, similar to the ones already executed when exposing the initial prototypes to the Internet, just to simulate what could happen and investigate whether the mitigation actions considered are of real use or not.

Questionnaires

At the current execution stage, no questionnaires have been sent yet to the participants. These surveys will be conducted once the initial stage of Pilot 1 comes to an end after a 3-month run, addressing the points considered as most relevant by the local partners in the consortium in charge of this Use Case. Through the participants' responses, it will be possible to acquire the overall feeling the service produces and take the actions required to deliver an improved version during the next piloting stage.

Summary – lessons learned, sustainability

So far, the most relevant lesson learnt relates to the difficulty to integrate a hardware-based security solution in the IoT devices. Another one relates to the relevance of the system delivering reliable data, which it seems to go hand to hand with the device locations and not exposing them in spots where the sensors may register erroneous values that would lead to incorrect measures.

Another lesson refers to the difficulty of getting people's interest and addressing citizens outside the technical environment and in the midst of this pandemic situation.

In what refers to sustainability, initial feedback provided by technicians close to Santander Municipality suggests it will be directly related to the reliability and usefulness of the data registered and offered by the sensors integrated in the IoT devices. In case they do not show a huge accuracy, credibility will go low and then no specific decisions will be taken based on this data.

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

This section describes the result of the Pilot 2, which will be the translation into real life of the ambitions sketched in Use Case 2.

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.

When we think about the current pandemic situation, there is a high concern and desire to keep the elderly and vulnerable people safe in their own homes in order to avoid emergency hospital admissions that are non-virus related.

Worldline proposes Senior Care, an IoT platform that allows users to be monitored by deploying a series of sensors for the home (bed occupancy sensor, door/window opening, movement sensor, etc.), as well as detecting emergency situations based on a series of previously configured rules and alerts, and thus giving immediate response. 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.

Senior Care Assistance provides the following features:

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

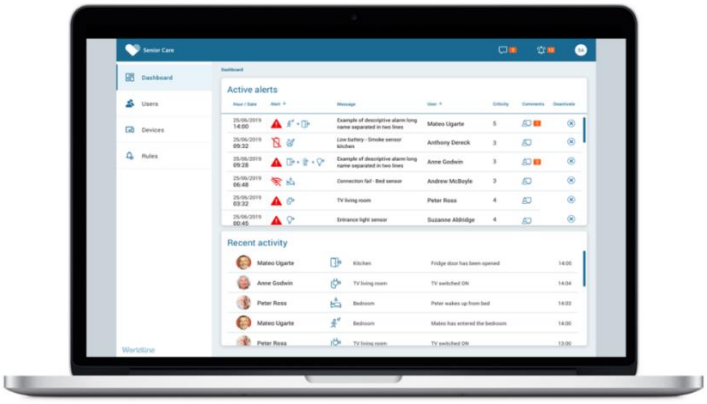


Figure 9. Senior Care Portal

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

- Improvement of quality of life of elderly people who live alone and are not familiar with the use of new technologies.
- Creation of a network of caregivers, formed by relatives or neighbours previously authorised by the elderly, who will be able to check users' status thanks to the combination of the measured parameters.
- Improvement of data gathering and information enrichment with the digital transformation of the current local tele-assistance & emergencies social service provided by the city government, through the introduction of digital sensors and communications.
- Improvement of data security and integrity through the use of M-Sec layers in the different elements that compound the service. For example, components such as the companion database with the quorum blockchain to prevent malicious attacks by a parallel encrypted system for data storage connected to the blockchain to ensure tamper-proof. A middleware between 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.

Challenges and mitigation actions on pandemic situation

With the objective to ensure that the pilot's phase takes place adequately and without major risks for any of the parties involved during the evaluation, the consortium has analysed the main challenges raised due to COVID-19 and the mitigations actions to be implemented to guarantee the results' evaluation.

One of the challenges faced in the current situation of COVID-19 is the possibility to go back to a lockdown scenario or the implementation of severe restrictions in terms of mobility, especially in what relates to the reduction of visits to elderly or vulnerable people and those considered of high risk. Evaluating all the components needed to run the solution, it could be that during the pilot phase, a sensor device was not working correctly and there was the need of replacement for a new one. In this scenario, a protocol is applied by the tele-assistance party to guarantee the continuity of the remote monitoring service following the guidelines established by the responsible official authority, restricting home visits to exceptional situations where the person's life is in danger.

Another challenge is related with the fact that tele-operators could not have enough time to use or test Senior Care as a parallel system to their current analogic solution due to the effects of the pandemic situation (i.e. extra work due to the COVID-19, possible sick leave of employees, etc.). On this scenario, 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 to attend Senior Care platform.

A final challenge raised is regarding the minimum number of participants to ensure that the sample of the results is enough to evaluate the M-Sec overall system. Even though the pilot consists of only five end users, the consortium has preselected ten additional users to cover a participant from the pilot eventually.

Table 4: Use Case 2 challenges and mitigations

Challenge	Description	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 paralel system to their current analogic solution	The teleassistance 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
4	Leaks of personal data may lead to lose the confident/trust from end users	M-Sec components integrated within the solution of 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.
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 replace the visit may not be possible…	A protocol is applied to guarantee the tele-assistance service 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 initially for 3 months but due to the informed consent signed with end users and contract with the teleassistance provider, pilot could be extended for longer than 3 months to guarante M-Sec components testing
7	Devices/solution is not working properly and data is not being reported correctly	Each day the teleassistance provider verifies with the user the status through a short call. All the alarms received are verified in addition with users.

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 Worldline as technological partner providing the solution, with Santander City Council easing the implementation in the city and 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, a training session has 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 with the pilot testing (i.e. new needs identified). Furthermore, in a weekly base, Atenzia sends Worldline a report with the major events or findings around the platform and the use of it.

Moreover, one workshop has taken place just one month after the initiation of the pilot, oriented to exchanging feedback on how the tool has worked so far (positive and negative things, things that are missing, etc.). The results can be seen in the figure below.

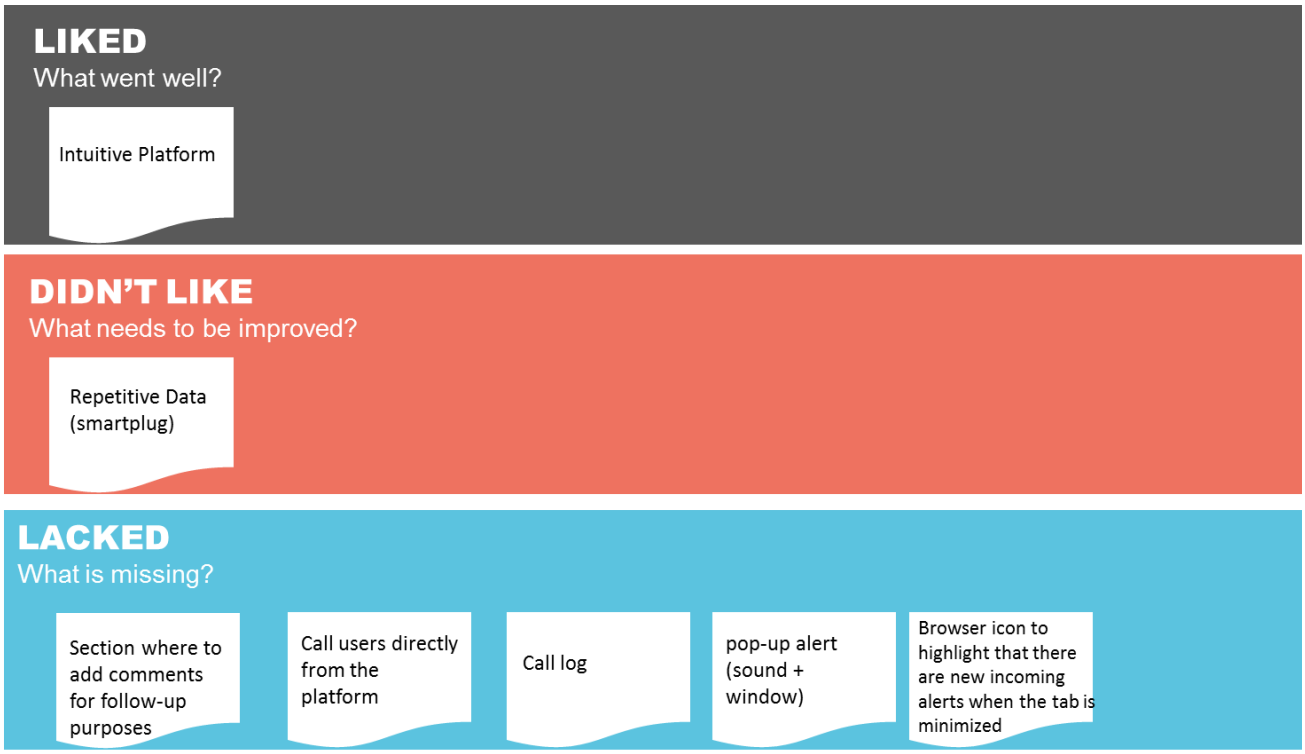


Figure 10. Workshop to evaluate the pilot test

Regarding end users, Atenzia counts with over 2000 users who are already part of the monitoring service. From this network, a total of 15 users were pre-selected during the months of January and February taking advantage of the regular visits to their homes. Due to the COVID-19, in May it was necessary to confirm the availability of the pre-selected candidates. During these individual visits, the pilot was explained to each one of the 15 tele-assistance service users, taking into account his/her profile and circumstances, with the aim of assess his/her degree of interest in taking part of the pilot. 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 as well as the informed consent provided. Each of the chosen users has different habits, in such a way it was possible to place the devices and configure the alarms in a more personalized way. For example, there were several users that the bed sensor was placed on the sofa where they watch television since the mattress was very 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.

Technical approach – M-Sec components

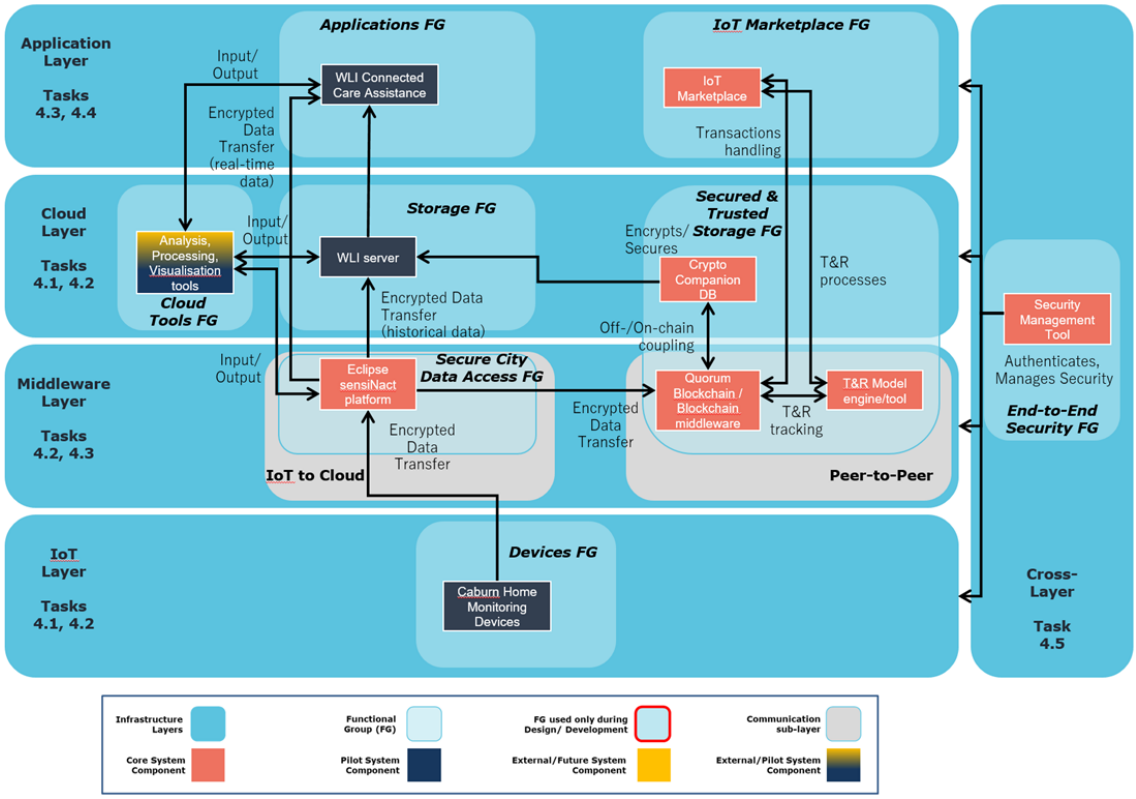


Figure 11. Use Case 2 Architecture View

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

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 12. 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 13. 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 14. 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 15. 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 is 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.

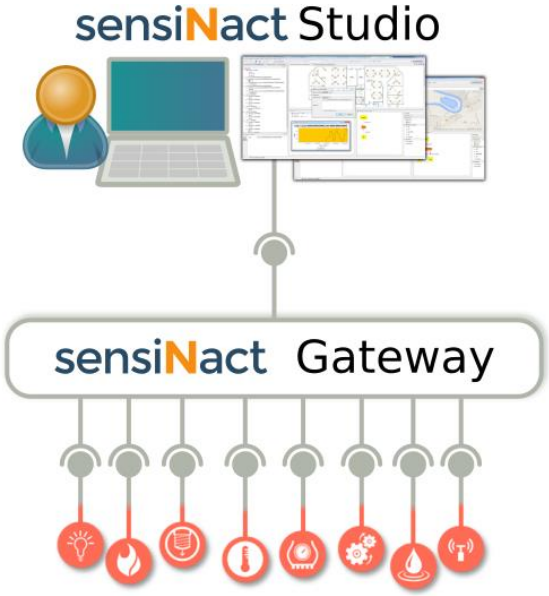


Figure 16. Eclipse sensiNact Platform

Once data is collected, it is 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.

Those data that it can be publically available because it doesn't contain any personal data related to the end user, is transferred to the M-Sec marketplace where stakeholders who may be interested on 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 the one of the data owner.

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.

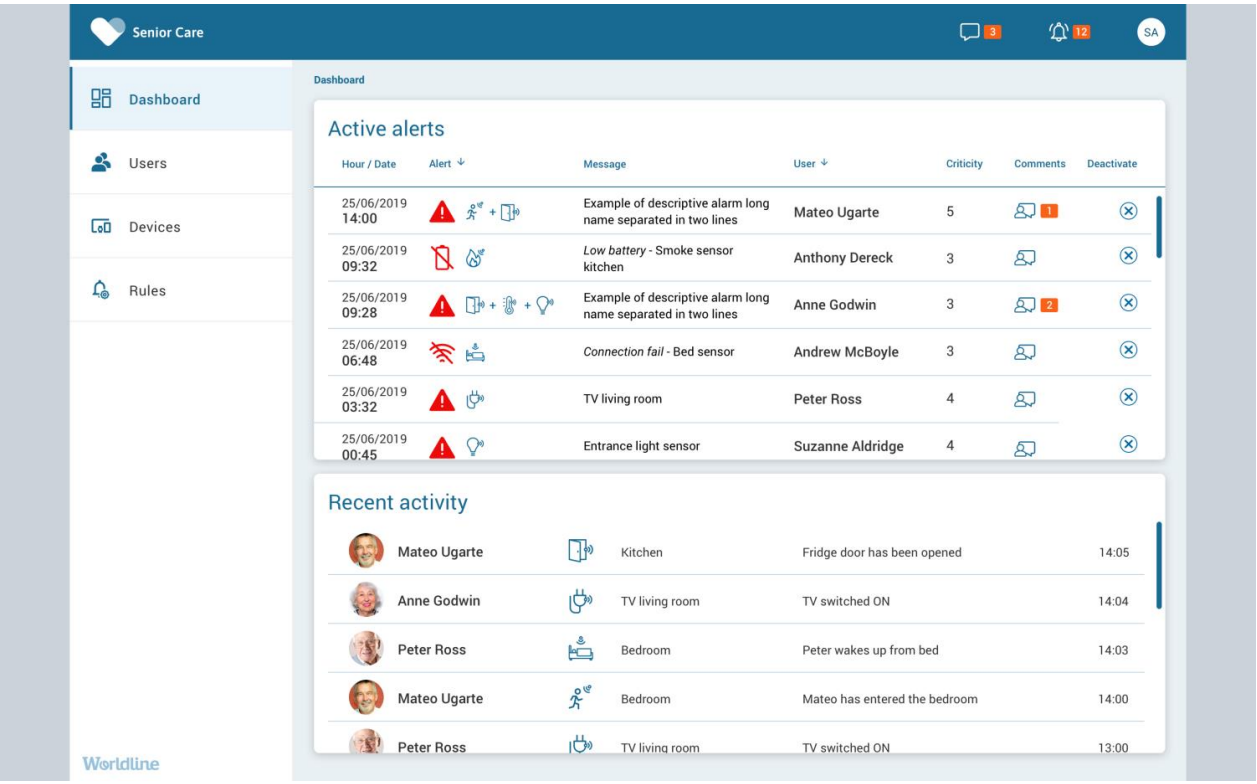


Figure 17. Dashboard Senior Care

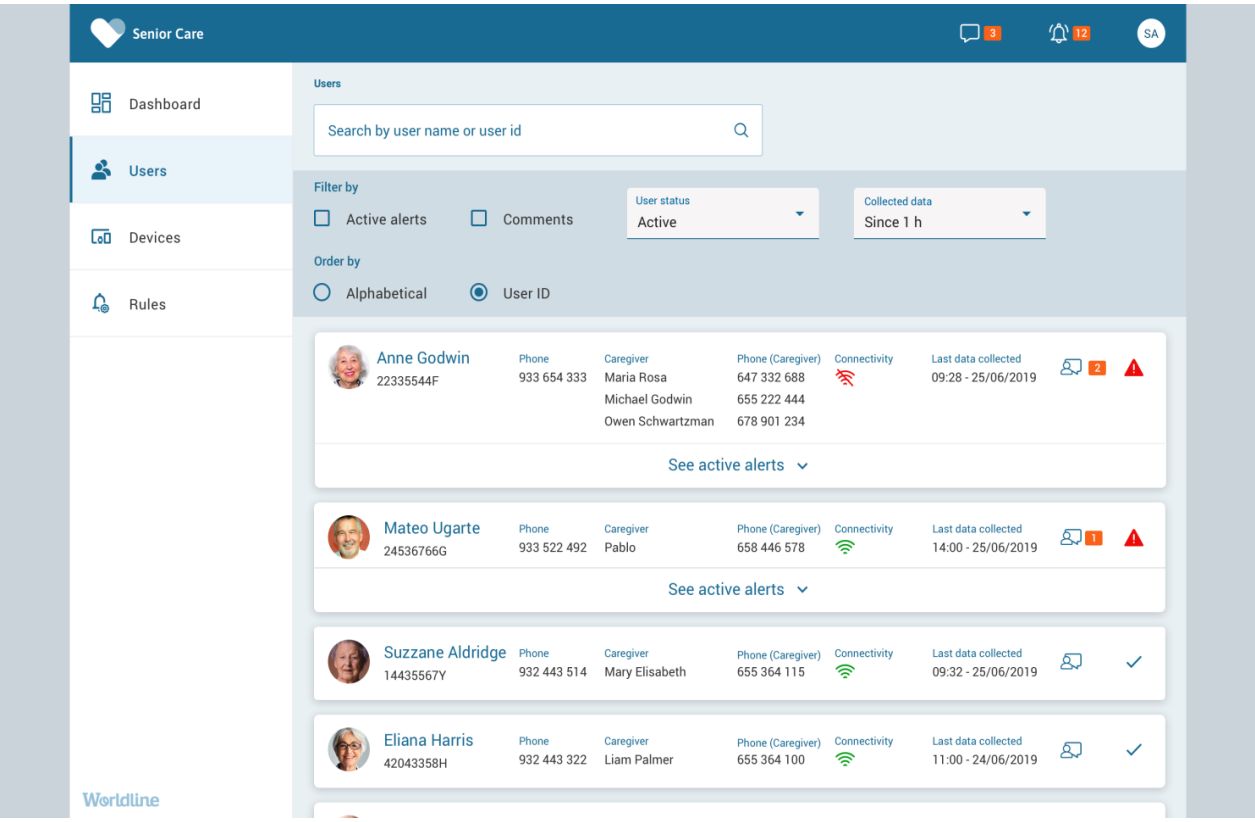


Figure 18. Users Management Senior Care

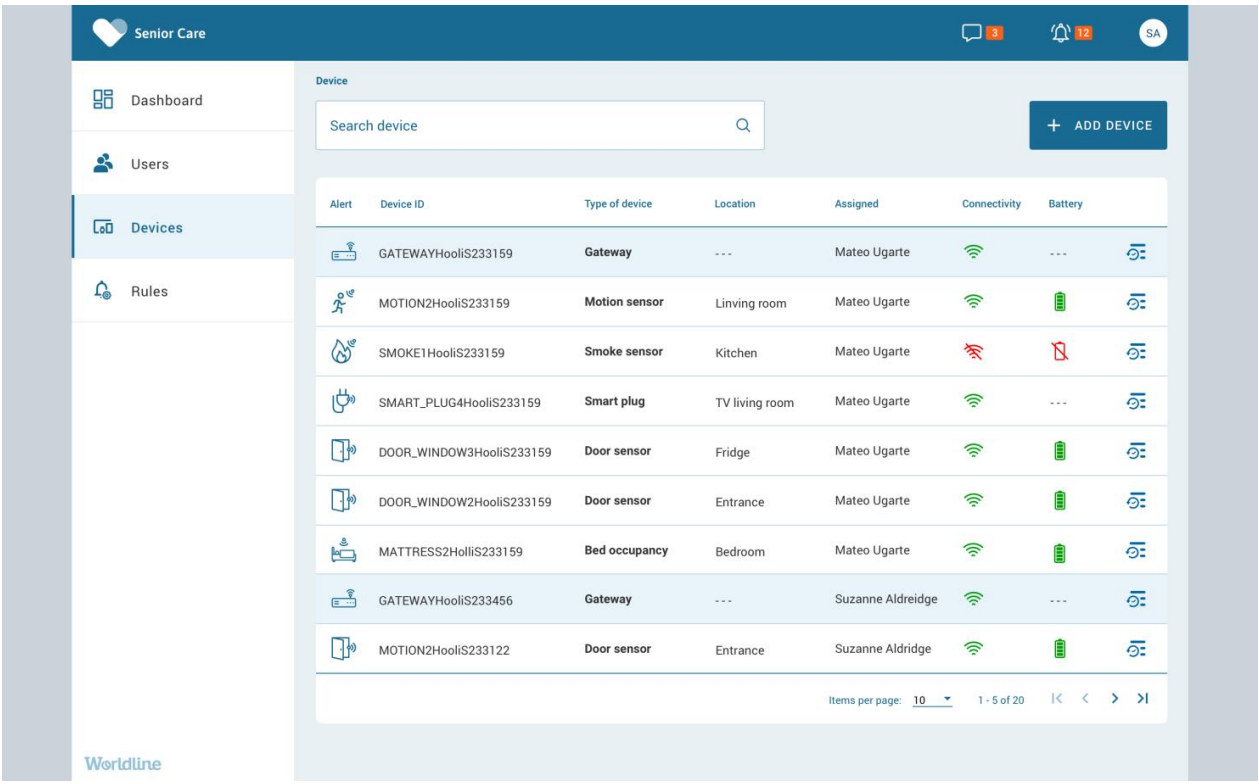


Figure 19. Devices Management Senior Care

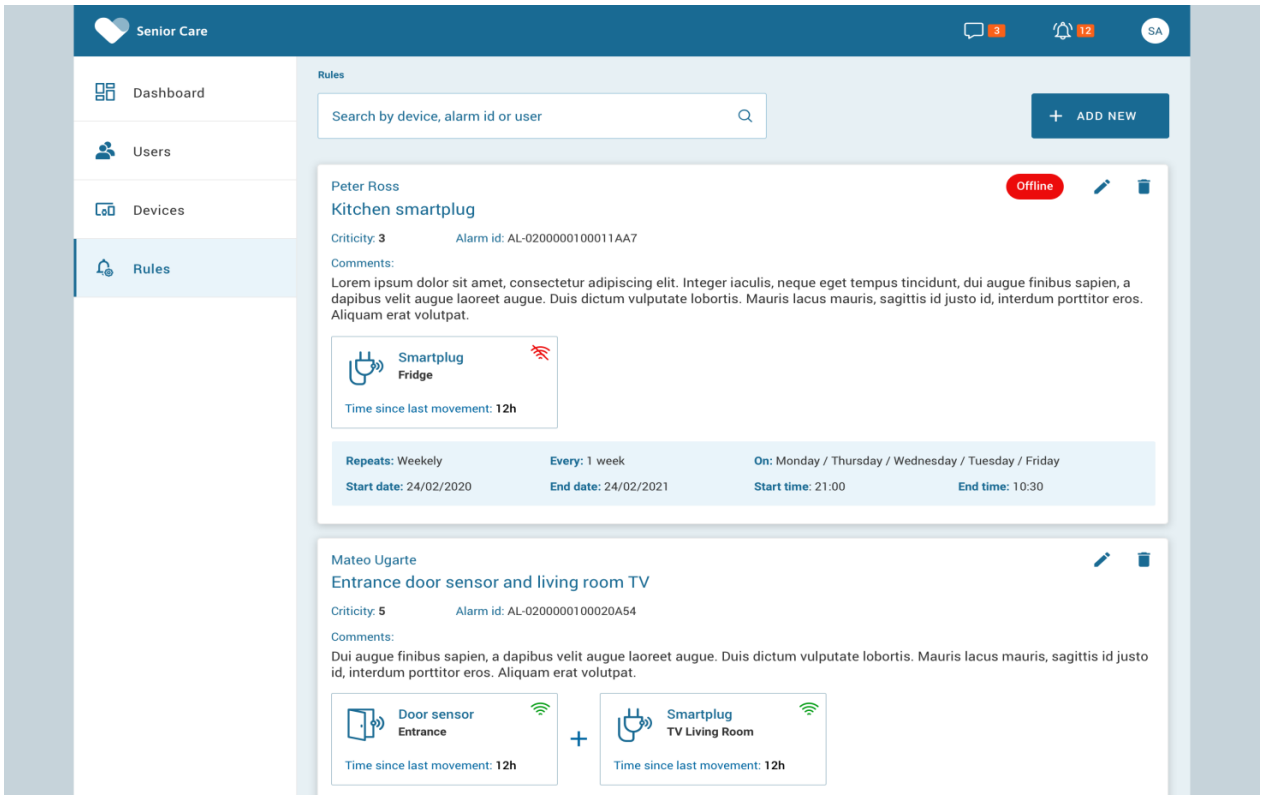


Figure 20. Rules Management Senior Care

KPIs and Evaluation

To achieve success, KPIs were defined in the previous version of the current deliverable submitted in July 2020. As not all the KPIs have been reached as the trial is still ongoing, we have updated only those metrics that could reflect the current status of the project:

Table 5: Use Case2 Pilot 2 KPIs

#KPI	Goal	How to measure?	Target Set	Target Achieved 1st Phase
#Participants	Minimum number of end users to test the solution provided.	Number of end users (ageing people) registered into the system	≥5 users	5
#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	TBD (applicable for a second pilot phase)	TBD (applicable for a second pilot phase)
#Data frequency	To evaluate speed at which new data is generated	Latency time	≤25s	Mean Latency 5sec. Frequency: events 235.659 generated-> 2618 events/day
#Events that have been handled during the length of the pilot	To evaluate the number of events raised and their reliability	Number of alarms that have been addressed	≥ 60 (4 alarms/month per user)	230 Alarms (based on more than 235,000 events)
#Data tampered	Verify data has not been modified	Thanks to Blockchain, sensitive data from this use case can be tamper proof due a hash pointer. The hash will indicate whether data has been modified. Worldline as owner of the solution provided to this use case, will try to modify data to check the vulnerability of the system and the validation of the hash function.	3 Attempts / 3 Detections	Too early
#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	Too early
#Data exchanged	To evaluate the	Transactions handled in the	>4 (1st Pilot	Too early

#KPI	Goal	How to measure?	Target Set	Target Achieved 1st Phase
	business value of the anonymized data sent from Senior Care to the M-Sec Marketplace	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	Phase) >20 (2nd Pilot Phase)	
#false positive events	Verify the reliability of the sensors	Manual way by verifying the reliability of the data with the end user	<5	1
#End points accessed	Higher number of end points higher vulnerability grade	Access log file	<10	Too early

Questionnaires

Taking into account the profiles of the participants in the pilot, two different surveys have been prepared and distributed: one for the teleoperators in Atenzia and another for the users of the teleassistance service. Both questionnaires can be found as annexes to this document, Annex1.

The first questionnaire consists of 20 questions and has been completed by two technical coordinators from the company Atenzia who are participating in the pilot.

The main results are listed below:

- They are quite satisfied with the ease of use and the Look and Feel of the solution provided, as well as the ease of installation of the home sensors at the user's home.
- They are satisfied in the way Senior Care has helped them to solve their problems, feeling safe using Senior Care as their current system, which can be complemented by the solution under test in this pilot.
- One of the survey respondents is quite satisfied with the ease of detecting a non-regular behaviour of a user through the alerts system implemented, while the other one considers that it is quite difficult.
- They are satisfied with the reliability of the information provided by the Senior Care system, as well as how this system and the M-Sec Project can help to reduce the breach about current security concerns in terms of data protection and increase user trust. In this sense, they would be interested in using Senior Care after the end of the test period.
- In assessing privacy in the use of Senior Care, one respondent is moderately concerned, while the other is slightly concerned.
- In terms of evaluating the accuracy of Senior Care compared to the current analogic system used by Atenzia, one of the participants is satisfied with the accuracy of the new solution, while the other is quite unsatisfied. In this sense, both of them report false detections related to motion sensors: some alerts for lack of movement, they contacted the user and it turned out to be false alarms.

Finally, both of them are quite satisfied with the collaboration with Worldline as the technical partner provider of Senior Care, with the solution itself, the technical support and the M-Sec contribution in terms of security.

The second questionnaire, consisting of five easy questions, has been distributed among the five eldest participants in the pilot: one woman and four men, two of whom are between 75 and 80 years old, while the other three are between 85 and 90 years old.

- Regarding safety, four of the participants reported feeling safer with the new sensors installed in their home while one of them reported feeling the same degree of security with and without the new sensors.
- In terms of Privacy, all of them agreed that none of them have felt their intimacy invaded at any time.
- All of them agreed that the installed sensors have not caused them inconvenience at any time, just as they thought it would not be necessary to add other types of sensors.
- Finally, they all answered unanimously that they would recommend this service to family and friends.

The procedure to test the solution implemented by Atenzia was to visit to end-users' homes, to explain the pilot, while the different sensors were installed and tested. On the one hand, end-users have shown their satisfaction and, without telling them anything, they knew how to test the devices. Additionally, the elderlies themselves were pleasantly surprised by the accuracy of the data retrieved by the sensors.

The main drivers for users to participate in the tele-assistance service offered by Atenzia are that they feel more secure, being more confident in certain situations, such as fainting, as they know that Atenzia is taking care of them.

Summary – lessons learned, sustainability

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

- Bed occupancy sensors were not working properly.
- As there is neither audio nor visual alarm, the Senior Care platform needs to be checked from time to time in order to know if any alerts have been issued.

In order to make the solution more practical for Atenzia, two issues have been reported:

- Add audio and/or visual alarm which informs tele-operator that there is a new alert on the Platform would be very helpful
- Add a module to visualise and analyse the statistics related to the tele-assistance service provided

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

This section describes the result of the Pilot 3 which will be the translation into real life of the ambitions sketched in Use Case 3.

Pilot scenario and objectives

UC3 is a pilot who 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 itself.

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 21: Mobile Sensing by 60 Gubage trucks in Fujisawa city

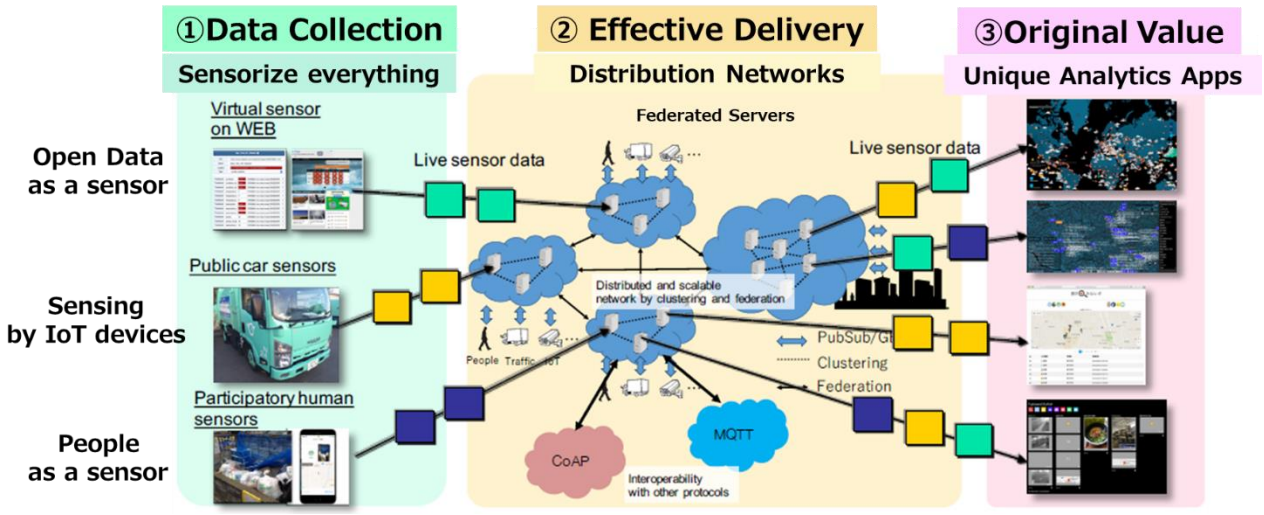


Figure 22: Keio mobile sensing platform based on SOXFire as IoT platform for Smart city

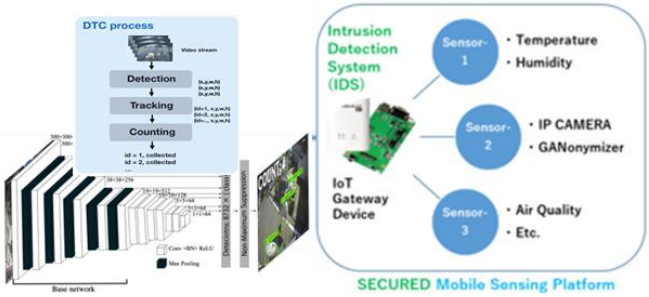


Figure 23: M-Sec Secure solutions which is integrated in Keio mobile sinsing platform

Challenges and mitigation actions on pandemic situation

As with other UCs as a whole, the fact is that there are major restrictions on conducting demonstration experiments themselves through actual IoT application services. Like other UCs, UC3, which uses cleaning vehicle sensing as an example, has issues such as implementation period and restrictions on verification organizations, but efforts to minimize the issues by devising test methods in a limited environment.

Table 6: Use Case 3 challenges and mitigations

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	Ensure that the UC can be tested for at least one month for 1st stage, then make improvements and re-test for a minimum of

Challenge	Description	Mitigation Action
	time for experiment.	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.

Technical approach – M-Sec components

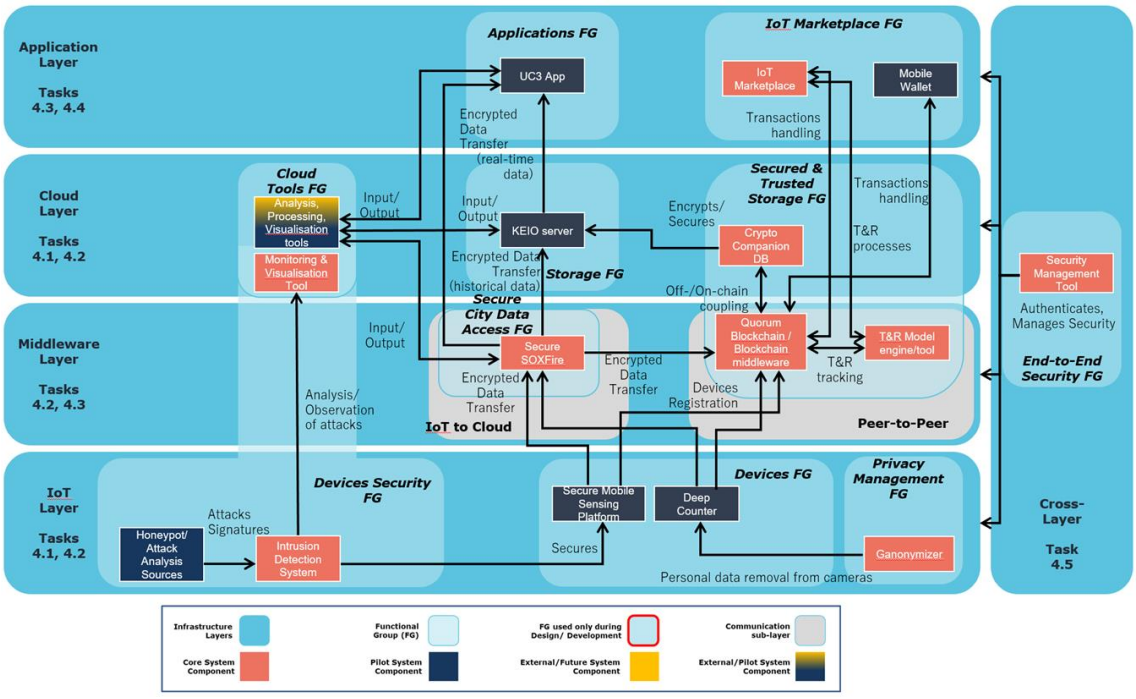


Figure 24. Use Case 3 Architecture View

UC3 Secure Mobile Sensing Platform will be realized by incorporating the security solutions of M-Sec project partners into the smart city platform centered on Keio SOX Fire, which has already been proven in Fujisawa city.

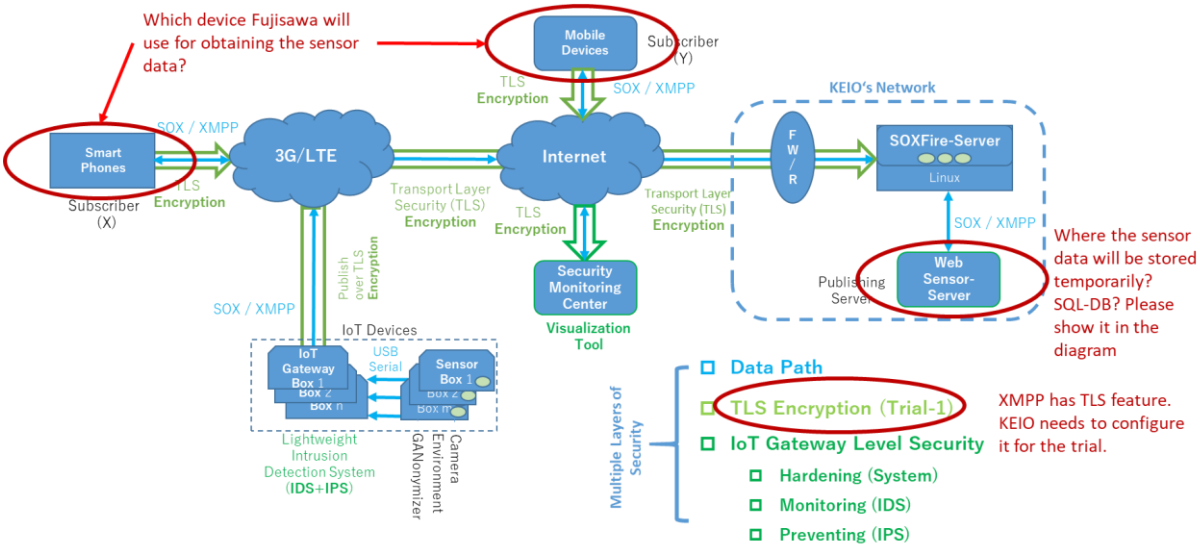


Figure 25. Mobile Sensing Platform integrated M-Sec secure solutions

KPIs and Evaluation

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 7: Use Case 3 Pilot 3 KPIs

#KPI	Goal	How to measure?	Target	Target Achieved 1st Phase
# platform users	Having multiple common platform users as a secure and trustworthiness mobile sensing platform.	Number of platform users	3	1 SmileCityReport
# Anonymization	Functional verification of privacy data protection	Number of privacy data erased from video data as privacy data protection	More than 20 privacy-related objects	8 GANonymizer used in SmileCityReport
# Secure Data Processing	Securely distributes data as a Secure Trustworthiness mobile sensing platform.	Number of data safely delivered as Secure Trustworthiness mobile sensing platform	More than 50 data	ongoing Deep Counter Honeypot
"Scan attempts	Hackers frequently scan the internet to find open	Using the security	90% or more	TBD

#KPI	Goal	How to measure?	Target	Target Achieved 1st Phase
blocked"	ports or services available on a device before an attack. Blocking scan can help reduce the attack surface.	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	Using the security monitoring tool	90% or more	TBD
"Telnet access blocked"	Telnet service is one of the highest exploited service for breaking into a device remotely. Blocking it would avoid such attacks.	Using the security monitoring tool	90% or more	TBD
“SSH access blocked”	SSH is another service that is commonly under attack to gain remote access to the controls.	Using the security monitoring tool	90% or more	TBD
"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.	Using the security monitoring tool	90% or more	TBD

Questionnaires

Unlike other UCs, UC3 is the platform itself, so we do not assume end-user questionnaires.

Summary – lessons learned, sustainability

At UC3, we conducted an actual verification using GANonymizer for privacy protection at a pilot event in Fujisawa City using SmileCityReport linked with UC4, but from the perspective of "Secure Mobile Sensing Platform" by integration of Security Asset of M-Sec partner, the actual pilot verification was not reached. However, since the integration is progressing, we will continue to study with the aim of pilot verification in the next stage.

Generally speaking, as pointed out in Gartner's Hype Cycle Report in 2020, IT technology related to measures against the COVID-19 pandemic that has changed the way of daily life around the world is an important position that requires immediate implementation. It is in. As mentioned earlier, UC3 not only means the original IT security by making full use of IoT in such a situation, but also secure to support various IoT application services in a non-contact manner to prevent COVID-19 infection. It is the IoT platform itself for smart cities.

Based on the garbage truck sensing in Fujisawa City, UC3 continuously aims to realize a secure IoT platform for smart cities, which is the purpose of the M-Sec project itself, through demonstration experiments of other UCs such as UC4 and UC5.

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

This section describes the result of the Pilot 4, which will be the translation into real life of the ambitions sketched in Use Case 4.

Pilot scenario and objectives

This 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 that let people (citizens and possibly additional visitors) to 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 metrology was yet to be explored, thus it is a 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 user's 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 next tit could be expanded to Santander, providing a cross boarder use case.

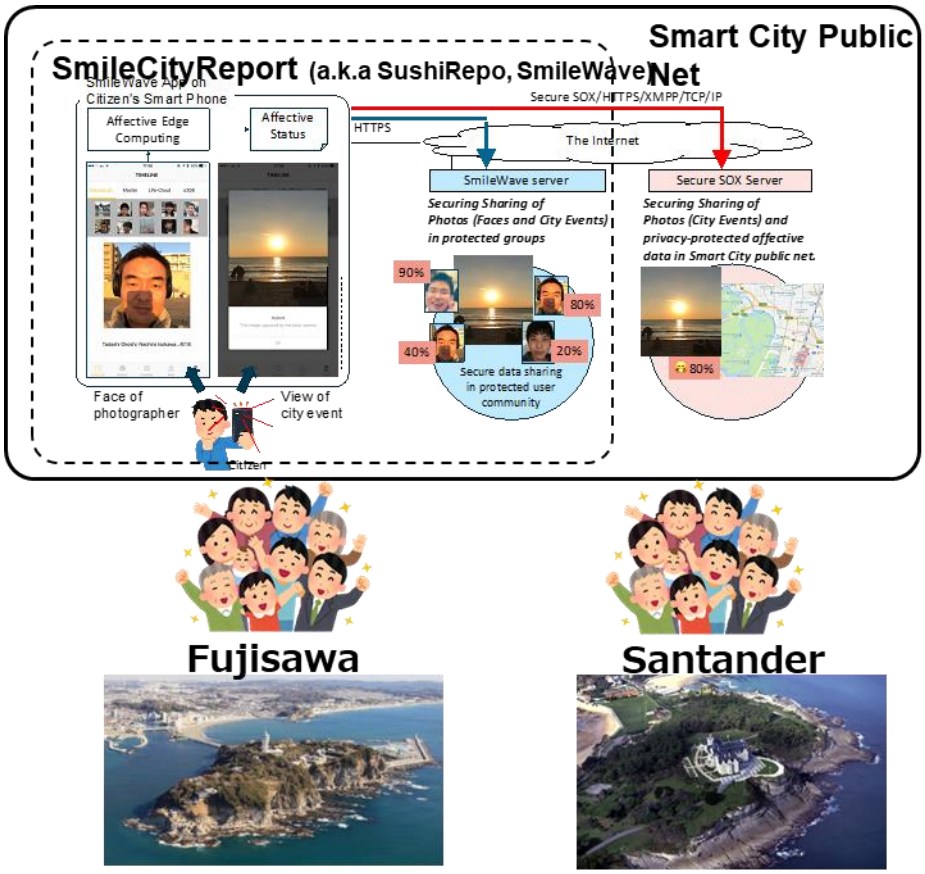


Figure 26. UC4 Overview

Challenges and mitigation actions on pandemic situation

In the severe situation of the COVID-19, UC4 first conducted 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 27. Fujisawa Jazz Meeting 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 28. 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
 メイン会場	What is the main venue like?	Please give us a report on the main venue! Please tell us about the groups currently playing at the main venue and the excitement of the venue! If you don't mind, please include your smile image!
 ストリート会場	What does the street venue like?	Please give us a report on the street venue! Please tell us about the groups currently playing at the street venue and the excitement of the venue! If you don't mind, please include your smile picture!
	Anxious artist	Please tell us the artists you care about! If you know, please tell us information about your favorite artists! If you don't mind, please include your smile picture!
	Nice restaurant, recommended mer	Please tell us a nice shop or recommended menu! If you don't mind, please give me your smile picture!
	Congestion situation	Please report the congestion situation! Please tell us about the congestion situation that everyone is interested in, such as enjoying Jazz with peace of mind! If you don't mind, please give me your smile picture!

Figure 29. SmileCityReport Themes for Fujisawa Jazz Meeting

The evolution of the COVID-19 in Santander has caused the cancellation or the indefinite delay of face-to-face events. For this reason, Santander City Council plans to organise a picture contest about several themes, such as virtual sightseeing and gastronomic experiences in the city, fostering the use of Smile City Report app. As this is a cross-border pilot, the idea is to synchronize the Santander picture contest with the event to be held in Fujisawa, if the evolution of the pandemic is better in Japan than in Europe.

As a first step before organising the photo competition, the SCR application will be tested internally in Santander, with the involvement of a group of friendly users, in order to detect and solve technical problems related to, for example, the mobile phone models or the operating system needed to run the SCR app, which may limit the number of participants.

Table 8: Use Case 4 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 to app store for iand google play for users to install SCR instead of test tools such as Test Flight.

Engagement process with citizens and stakeholders

Many reports were actually posted by participants on the five default themes mentioned in the previous section. An example is shown below as a screen example of Smile City Report.

Figure 30. Posted Report from users via SmileCityReport

Technical approach – M-Sec components

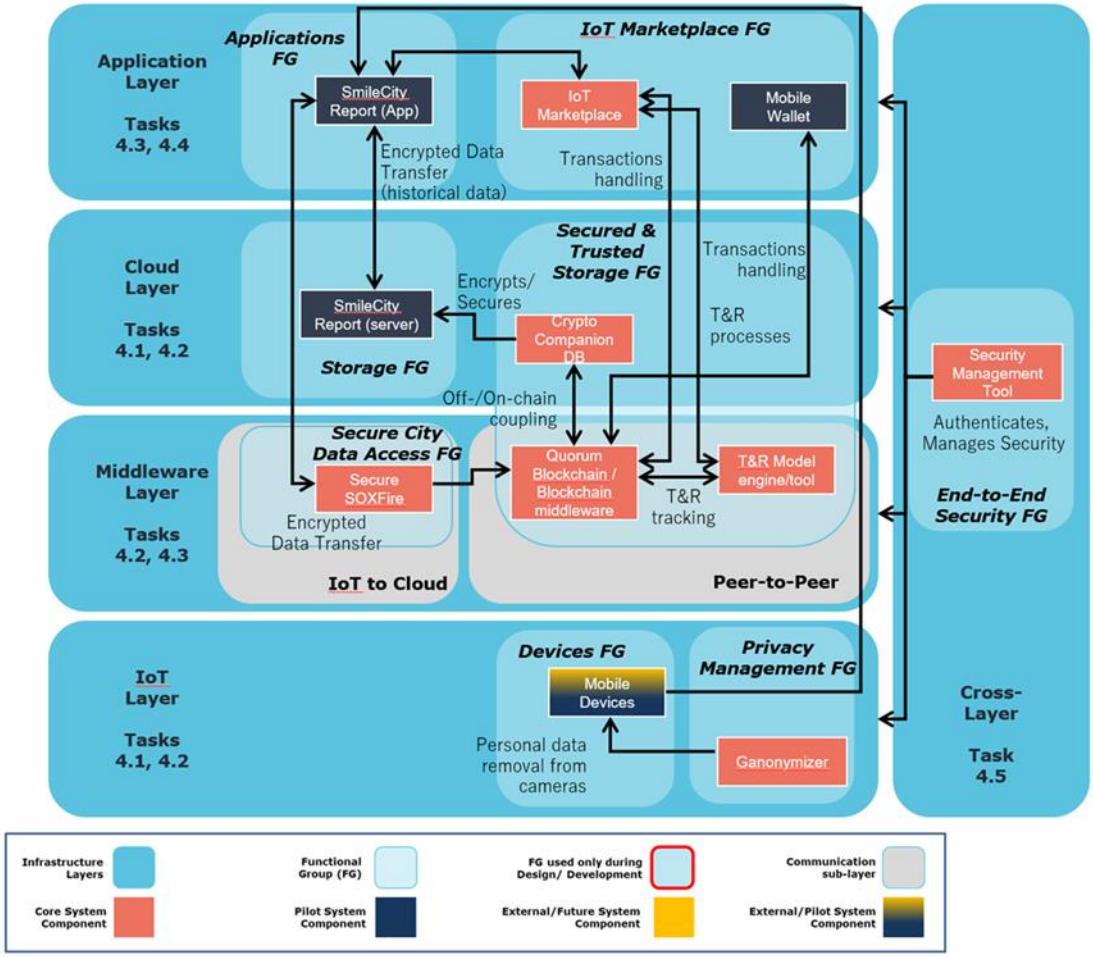


Figure 31. Use Case 4 Architecture View

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 Market Place 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" that automatically erases privacy-related information from camera images used at various sites in smart cities by image processing using deep learning. An example of the venue image actually taken at this demonstration site is shown below.

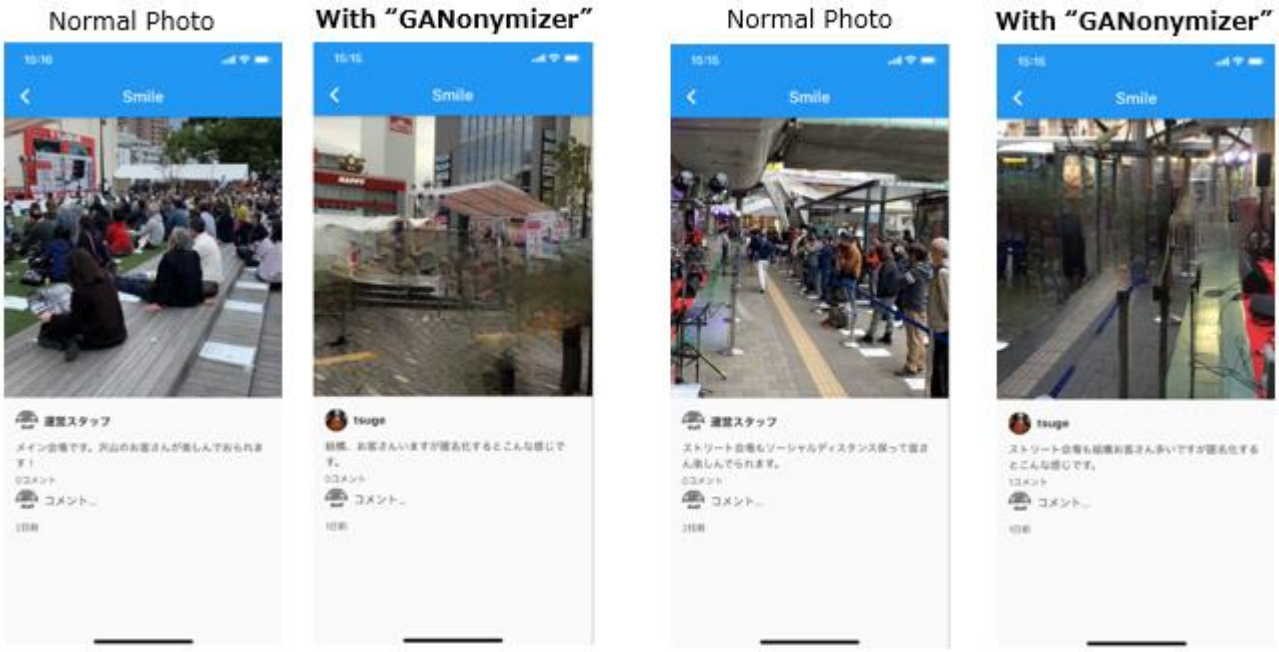


Figure 32. Automatically Privacy Data Protection by GANonymizer

KPIs and Evaluation

The table below shows the number of reports actually posted at the "Fujisawa Jazz Meeting" mentioned up to the previous section, and reports using GANonymizer.

Table 9 Actual number of reports by user

SmileCityReport trial at Fujisawa Jazz Meeting			
Theme	# of Psted Repors	# of following comments	# of GANonymizer
Thenme for testing	6	1	1
Congestion Status	23	1	5
Recommended Restaurant	7	4	2
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	84	8	8

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

Table 10. Use Case 4 Pilot 4 KPIs

#KPI	Goal	How to measure?	Target	Target Achieved 1st Phase
# of privacy-related objects filtered out from input images	To evaluate the volume of data from which privacy-related objects have been filtered out	Counting the number of processed images in the component.	More than 70% of the objects that the filtering component originally targeted.	More than 70%
# of objects going to SecureSOXFire	To evaluate how much data objects to be input into the public smart city network	Number of data (post object)	100	84 Strictly speaking, the integration of Keio SOX Fire and Smile City Report is a provisional version.

Questionnaires

The questionnaire carried out during the event "Fujisawa Jazz Meetin' 2020", which can be consulted in the Annex1 of this report together with the main results, includes four different topics:

- Shonan Fujisawa Jazz Meeting event,,
- SmileyCityReport app,
- Privacy protection tools,
- Other questions, generic questions related to.

Summary – lessons learned, sustainability

As mentioned above, the first trial using the beta version of Smile City Report was actually held at the "Fujisawa Jazz Meeting" event held in Fujisawa City on November 7, 2020. By actually having the users use it, the following issues were concretely found.

-It is difficult for the user to understand how the in-camera image is taken from the viewpoint of the user interface.

-Compared to the iPhone version, the Android version had a problem that depended on the terminal at the time of installation, and it was necessary to deal with it on site.

-The privacy protection GANoymizer was very effective and had an effect exceeding 70% of the target, but future measures are required for the remaining images.

Although there were issues to be examined as described above, by actually setting a theme that matches the citizen event of the Smile City Report of UC4, it will be positioned as a valuable first step for the Cross Border Trial in collaboration with Santander in the future.

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

This section describes the result of the Pilot 5 which will be the translation into real life of the ambitions sketched in Use Case 5.

Pilot scenario and objectives

This pilot is a cross border trial, which will be 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. More information is available in D2.3 and this pilot will be implemented in 2021.

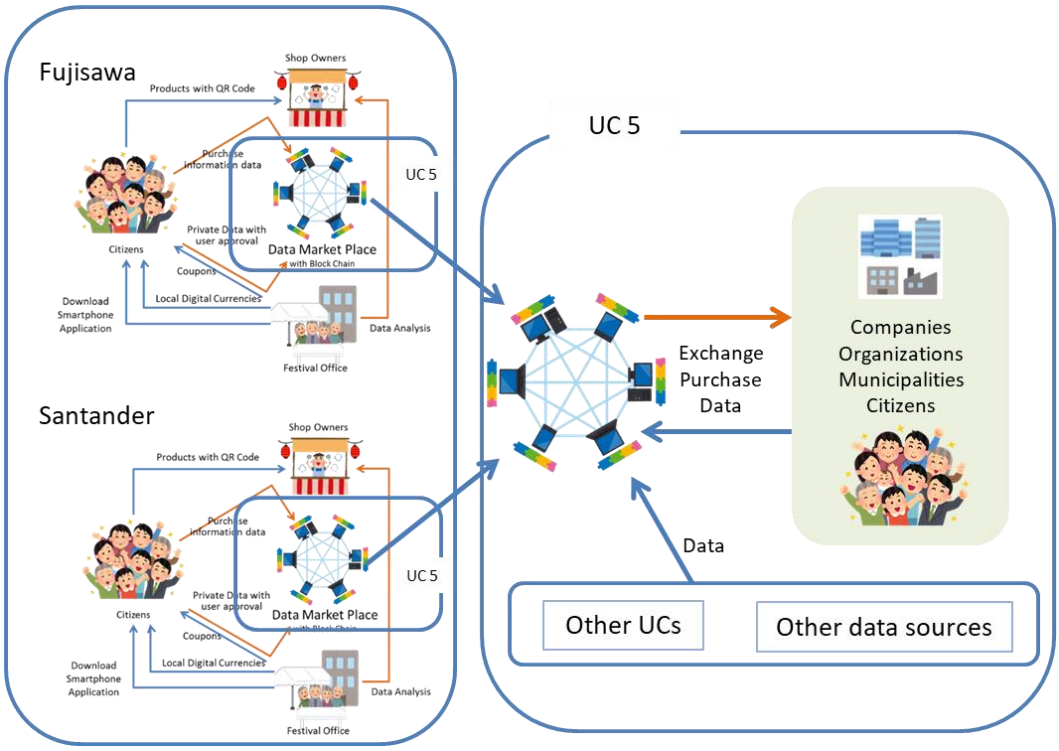


Figure 33. UC5 Overview

Challenges and mitigation actions on pandemic situation

The initial plan was to recruit participants by coordinating with events in Santander and Fujisawa, by introducing the project at exhibitions, by holding seminars and so on. However, due to the pandemic situation, almost all events such as exhibitions and seminars where people gather have been cancelled or postponed. Currently, the project is considering recruiting participants by the following methods:

- Introduction of data marketplace by webinars and asking for participation in the trial
- Introduction of data marketplace to other pilot participants at the same time
- Asking for participation of stakeholders and related parties

In recent months, at least in Japan, the number of people infected with COVID-19 has been stable, and various events have tended to resume. However, as the number of infected people has increased again recently, it is predicted that events will be postponed or cancelled. The number of infected people in Europe is far higher than that in Japan, and lockdowns and requests to refrain from going out are being issued one after another in major European cities. Collaboration with events where people gather can no longer be expected. The methods listed here are considered on the assumption that they will be implemented virtually, but if a pandemic situation reduces people's motivation to participate in new events, it might not be possible to attract participants as expected. This remains a concern for the Field Trial implementation.

An additional measure which is under consideration by the consortium is to provide free tokens to Marketplace users, as a way of making their participation more attractive.

In terms of privacy, no personal data is requested at the registration stage, only an identifier and a password. Moreover, after analysing the data of each pilot to be integrated, it can be assured that no personal data will be transferred to the Marketplace. Therefore, there will be no risk related to data store or exchange (off-chain).

With regard to contents, the consortium considers that it is technically possible to provide tools to control the data that could be uploaded by stakeholders to the Marketplace.

Table 11: Use Case 5 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	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)
6	Control data uploaded by stakeholders	Technically it is possible to add control

Engagement process with citizens and stakeholders

Regarding the data marketplace, we will request cooperation from M-Sec stakeholders to try it out. In addition, we are considering asking UC4 participants to cooperate by introducing the data marketplace at

the same time as trying out the Smile City Report because UC4 is relatively easier to reach to participants. Details are under consideration in the future.

Technical approach – M-Sec components

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 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

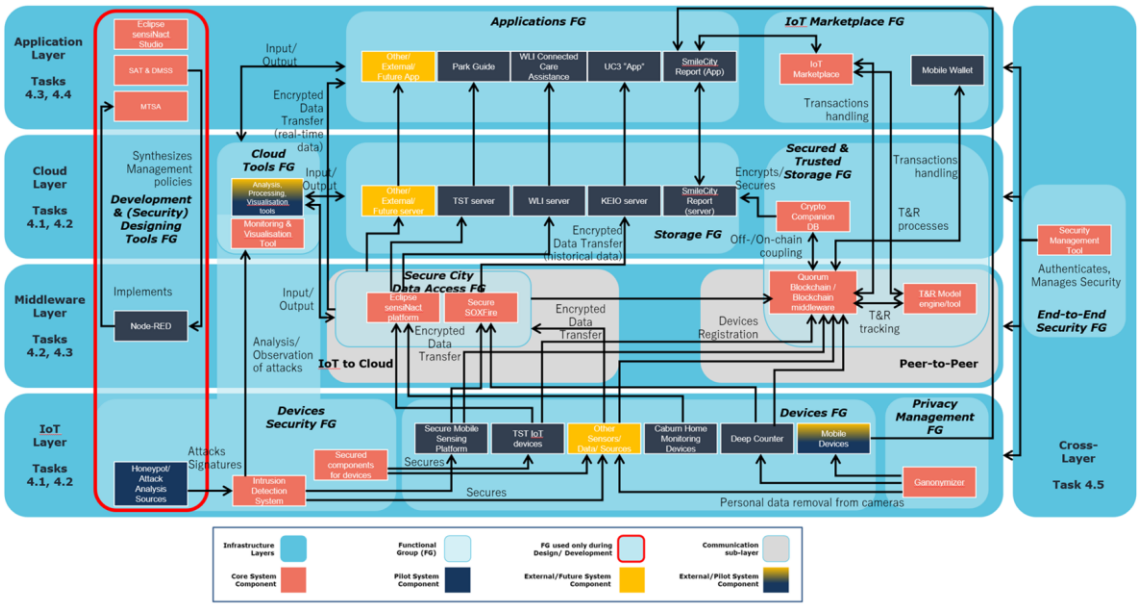


Figure 34. M-Sec Architectural view

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.

Integration between IoT Marketplace & SOXFire

For the purposes of integration of IoT Marketplace and KEIO SOXFire, a new module was developed named “IoT Marketplace – KEIO SOXFire Bridge”. This module consists of the parts: the KEIO SOX-store and ICCS Proxy Server.

This integration allows us to handle big volumes of sensors and data. As a result, numerous sensors handled by KEIO SOXFire can be registered in the IoT Marketplace and their data are available for purchases by potential buyers. As shown in the following figure of the overview of this integration, it is possible to show in the dedicated created User Interfaces of the Marketplace all the available sensors in real time.

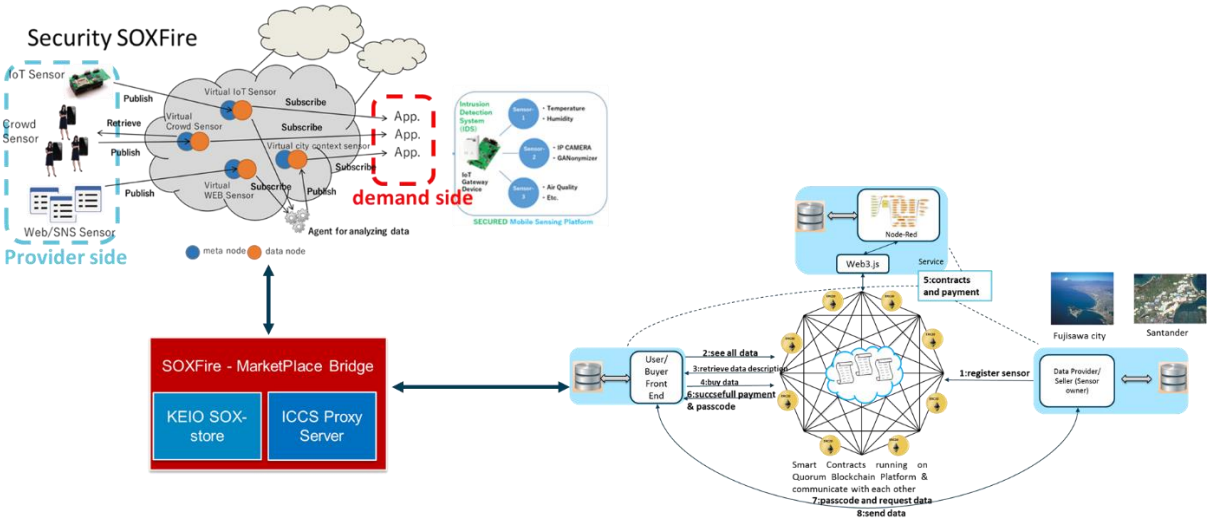


Figure 35. Overview of the integration between IoT Marketplace and SOXFire

The user is able to see all the available sensors and purchase data of interest after specifying the required details such as the time period of interest. Upon successful purchase, M-Sec Tokens are transferred, and new transactions are stored in the blockchain. Implementations of the IoT Marketplace and Middleware ensure that only after having sufficient funds and exchanging their value by paying, the buyer is able to see the purchased data. It is important to notice that through the implemented “IoT Marketplace – KEIO SOXFire Bridge”, data are coming in real time from the sensors to the buyers.

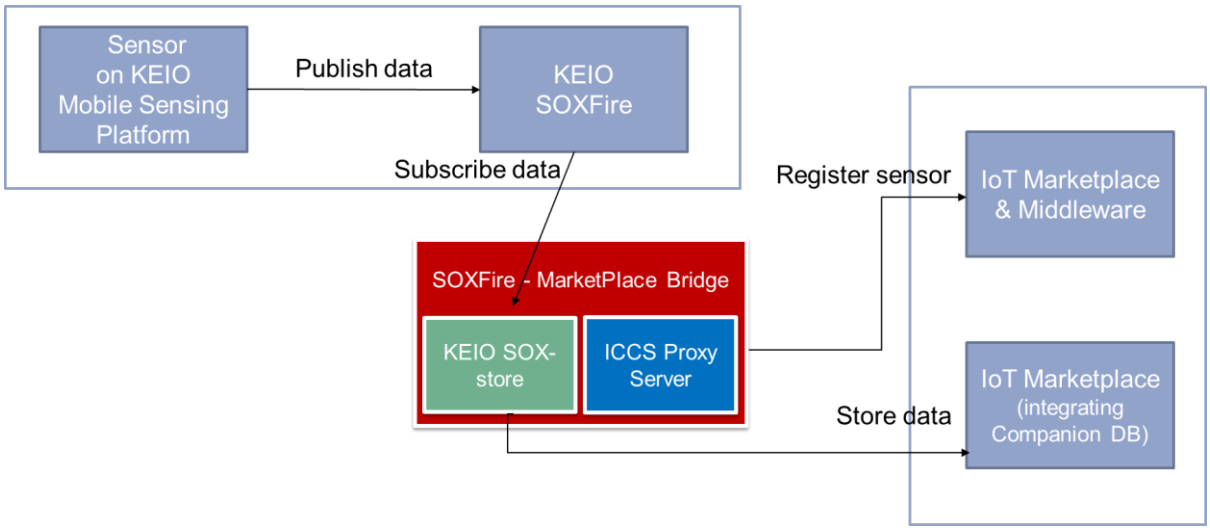


Figure 36. Technical details of the IoT Marketplace-KEIO SOXFire Bridge

Integration between IoT Marketplace and Smile City Report Application

The integration among IoT Marketplace and the Smile City Report Application facilitates the access of end users to M-Sec services. In this context, users are able to upload photos and specify the theme they belong into. Similarly, stakeholders, potential buyers, are able to get informed about the uploaded content. The following Sequence diagram depicts the interactions in a technical level among the Smile City Report App, the IoT Marketplace, the Middleware Services, IPFS, and end users who have access to the services provided by M-Sec.

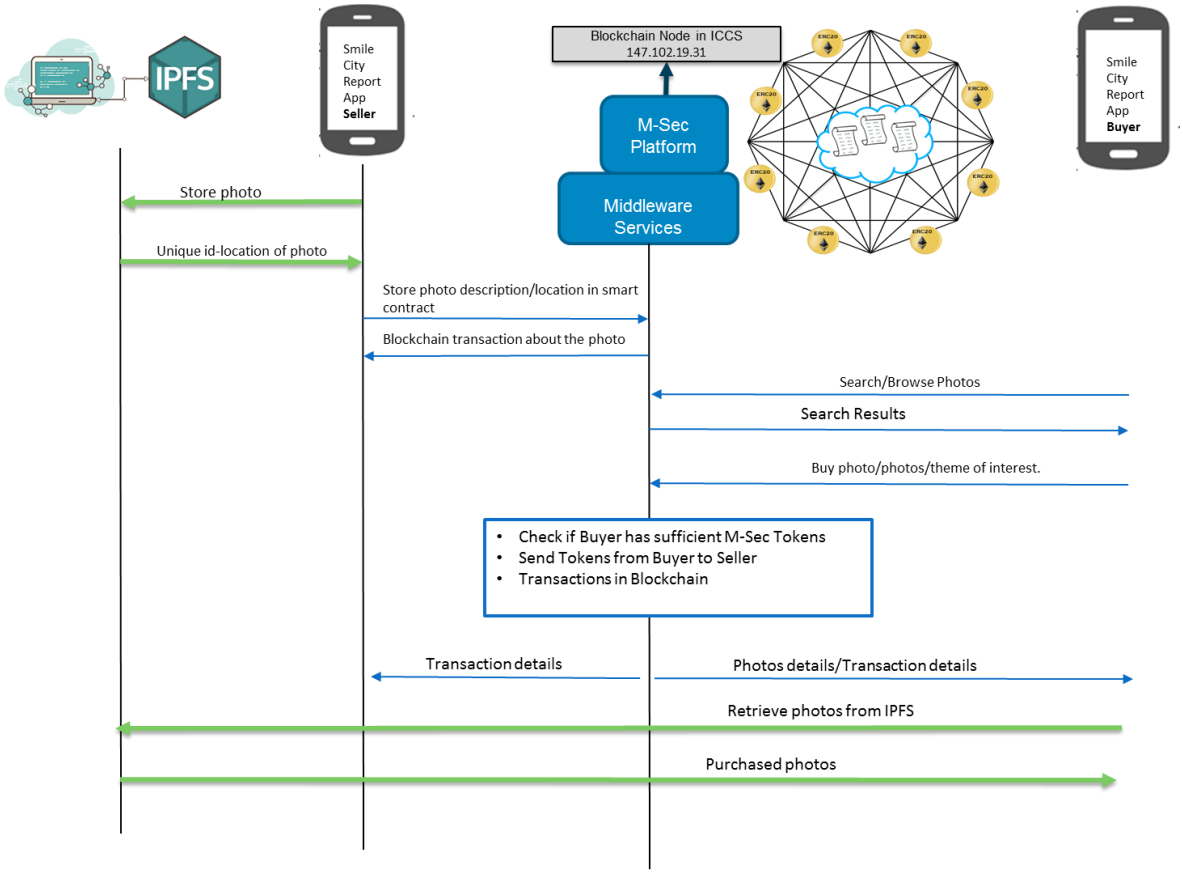


Figure 37. Sequence diagram

Integration between IoT Marketplace and Quorum Blockchain

In order to build marketplace where data collected during field trials can be traded in both Japan and Europe while ensuring security on all layers, we integrated IoT Marketplace with Ethereum-based Blockchains. Various smart contracts have been implemented, written in Solidity programming language, allowing the registration of new users, registration of sensors, exchange of data with our M-Sec Token, Know your Customer mechanisms, handling of smart cities sensors and data and more. User Interfaces were developed based on modern technologies and techniques and using libraries such as Web3.js that allow the interaction with Blockchain and smart contracts deployed.

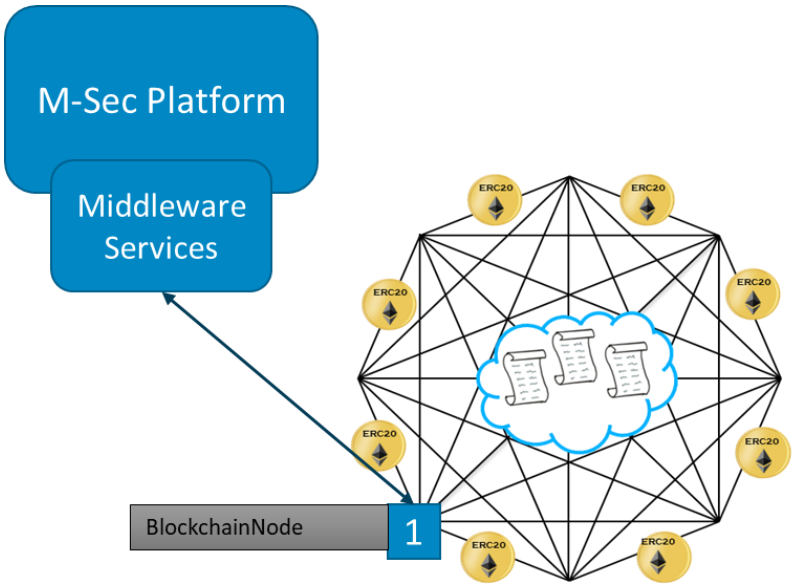


Figure 38. Overview of M-Sec platform and Middleware Services interacting with Blockchain

Integration between IoT Marketplace and Mobile Wallet

For the purposes of integrating a Wallet with the IoT Marketplace, different solutions have been examined or developed. The integration of Metamask, which is a browser plug-in, allowed many features of the marketplace to be more securely provided. As a result, user could “sign” all his/her transactions, users could verify their identity in order to have access to the data they have provided or have purchased and the Marketplace could allow only to buyers, who have actually paid, to be able to see the data.

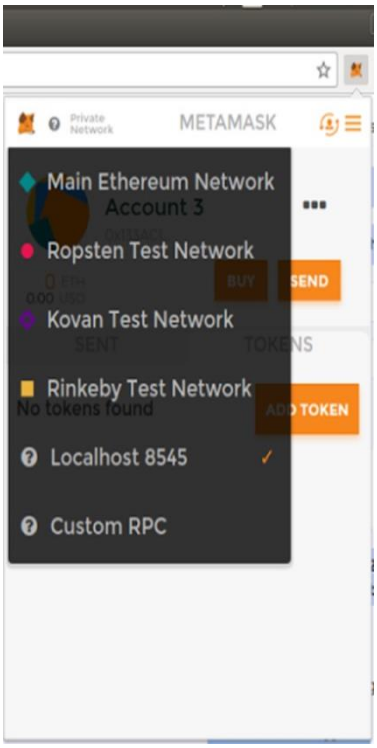


Figure 39. Screenshot of Metamask

Another solution examined was the Ethereum Wallet, which allows the users of the IoT Marketplace to watch the smart contracts of interest, perform transactions, send Tokens and more.

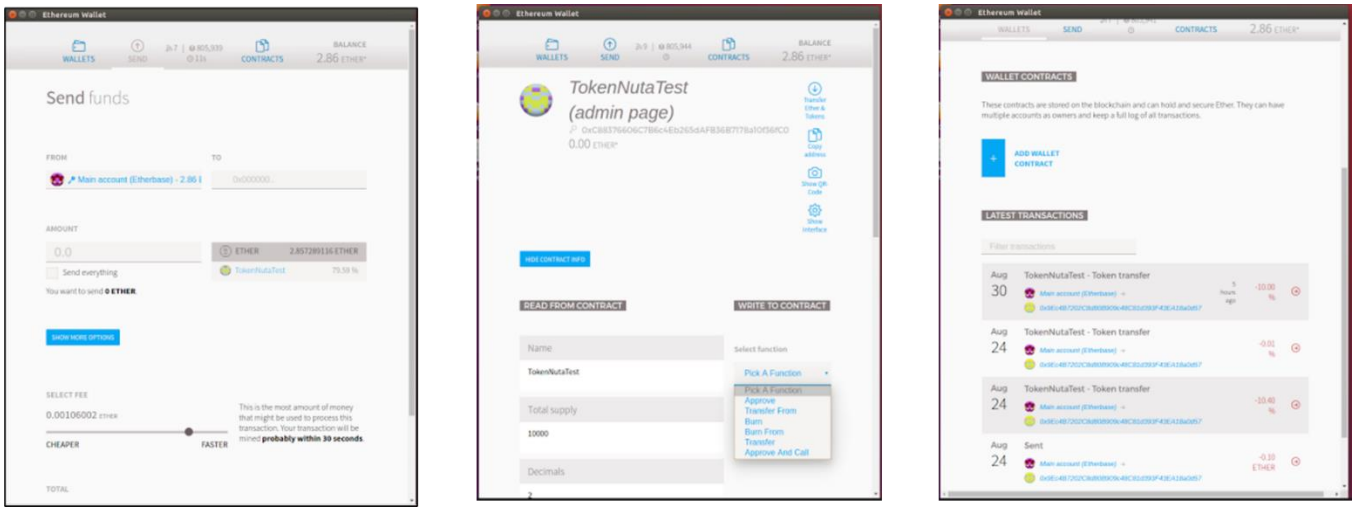


Figure 40. Ethereum Wallet as a way to connect to an Ethereum-based blockchain network

Integration between IoT Marketplace and Node-Red

IoT Marketplace has been integrated with Node-Red. Many flows were creating handling the interaction with the user, deploying smart contracts to the blockchain and interacting with them. As a powerful visual

tool that allows the integration of different components, tools, APIs into a common application, Node-Red and the flows we developed on top of it allowed us to handle sensors and data and visualize respective information to the end users.

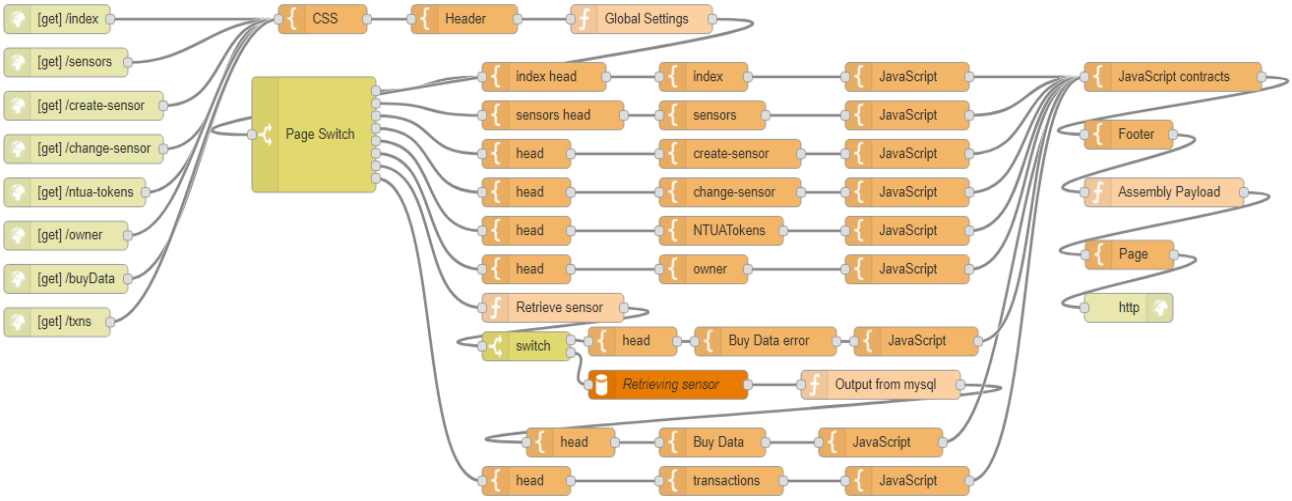


Figure 41. Node-Red flow supporting the interaction of end users with IoT Marketplace

Different interfaces have been developed. In the following Figure, we can see the integration of maps within the Marketplace, enhancing the visual representation of sensors to end users.

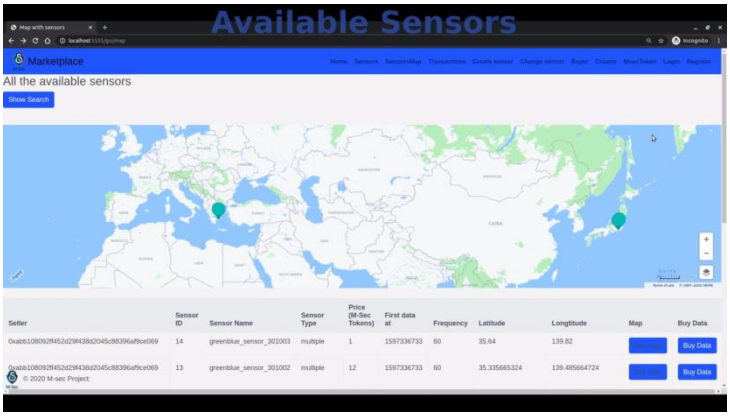


Figure 42. User Interface displaying the registered sensors

Similarly, the user is able to search over all the available sensors as shown in the Figure below, by filling the fields in the forms such as the area, the type of the sensors (e.g., temperature, pressure, etc.) and frequency of measurements (measurements/hour).

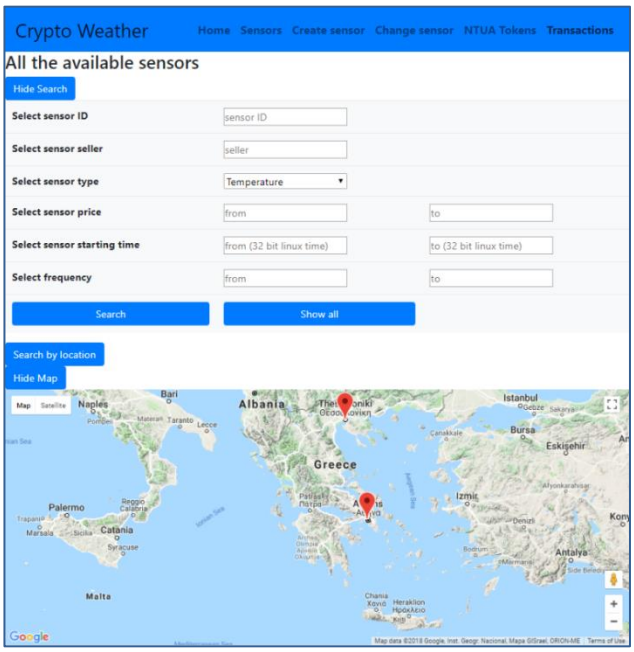


Figure 43. User Interface displaying sensor information

KPIs and Evaluation

This section will be filled in D2.4.

Questionnaires

This section will be filled in D2.4

Summary – lessons learned, sustainability

The main goal of UC5 is to set up a secure data marketplace, and the field trial will be based on exchanging the data collected in UC1 to UC4, and will be provided while organizing the information obtained by network sensors. However, as repeatedly stated in this deliverable, the spread of COVID-19 infection has postponed field trials of other use cases, and inevitably delays data collection. In the meantime, we are proceeding with the technical integration of M-Sec assets and tools for the data marketplace, and that is the main report in this deliverable. We are planning on starting field trial of UC5 in early next year, but it will be decided depending on various circumstances.

3 Conclusions

This document provides a report of M-Sec initial pilots, detailing the main activities carried out in Santander and Fujisawa. It was concerned that it might be challenging to implement all of the pilot plans as planned originally nor the project cannot implement even one pilot when COVID-19 infection started. However, in such a situation, we are proceeding with those implementations step by step with the cooperation of various stakeholders. We have decided to extend the project period, so all the members are working together to achieve as many project goals as possible.

As stated in each section of the Use Cases, we are also considering changing the plan according to the situation. Especially for pilots other than UC3, citizen participation is a prerequisite, therefore it may be necessary to further plan revisions depending on the future world situation. The major issues of the pilots are how to solicit the participation of citizens and companies in a virtual environment, and how many participants we can conduct for demonstration experiments. In the pandemic situation of COVID-19, there are increasing opportunities to hold events remotely using the Internet, so virtual security, which is the main research purpose of this project, is a noteworthy issue. We will proceed with the project while incorporating the opinions of various stakeholders.

Annex 1 – Pilot Questionnaires

Pilot2 Questionnaires

First phase questionnaire (after launching Connected Care) to teleoperators from the tele-assistance company testing the "Home monitoring security system for ageing people".

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 Connected 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 Connected 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 Connected 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 Connected 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 Connected 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 Connected 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 Connected 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 Connected 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.

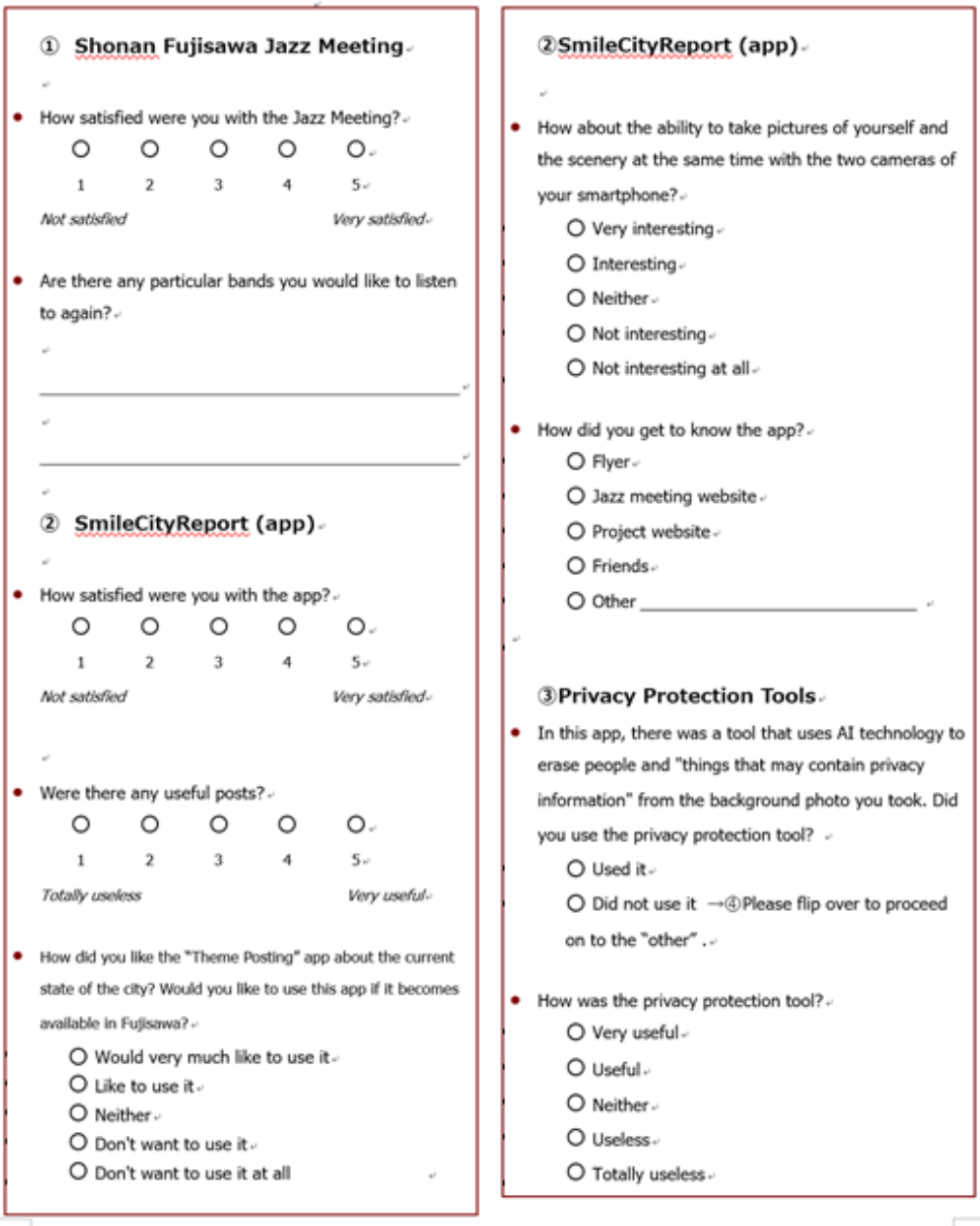
18. How would you assess the collaboration with Worldline as the technical partner provider of Connected Care? *(From a scale from 1 (very unsatisfied to 5 Very satisfied)*
    1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐
19. Please, rate your overall satisfaction with the solution itself, the technical support and the M-Sec 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).

…….

First phase questionnaire (after launching Connected Care) to users of the tele-assistance service testing the "Home monitoring security system for ageing people".

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 ☐

Pilot4 Questionnaire & results



① Shonan Fujisawa Jazz Meeting

- How satisfied were you with the Jazz Meeting?
  1 2 3 4 5
  Not satisfied *Very satisfied*
- Are there any particular bands you would like to listen to again?

② SmileCityReport (app)

- How satisfied were you with the app?
  1 2 3 4 5
  Not satisfied *Very satisfied*
- Were there any useful posts?
  1 2 3 4 5
  Totally useless *Very useful*
- How did you like the "Theme Posting" app about the current state of the city? Would you like to use this app if it becomes available in Fujisawa?
  - Would very much like to use it
  - Like to use it
  - Neither
  - Don't want to use it
  - Don't want to use it at all

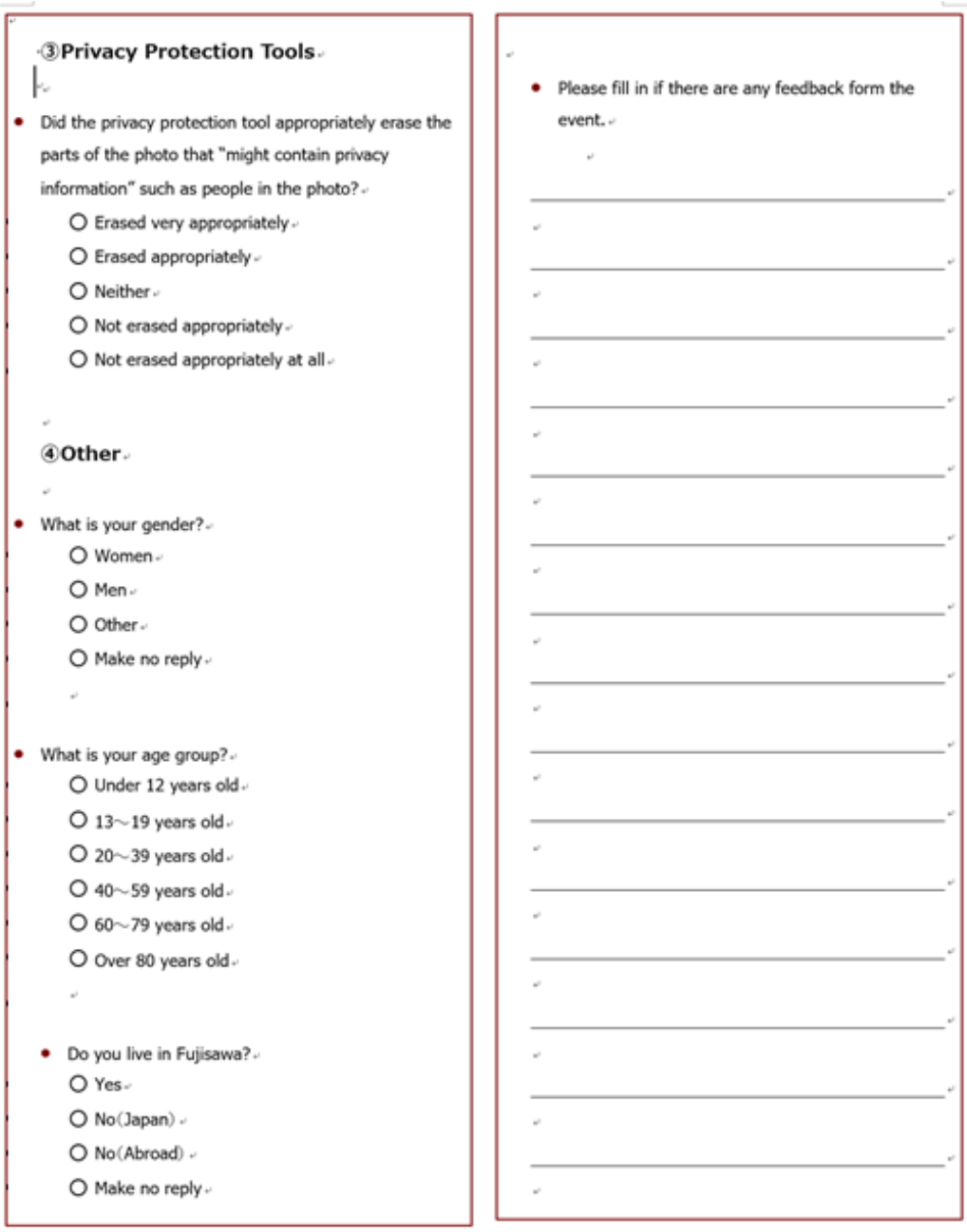
②SmileCityReport (app)

- How about the ability to take pictures of yourself and the scenery at the same time with the two cameras of your smartphone?
  - Very interesting
  - Interesting
  - Neither
  - Not interesting
  - Not interesting at all
- How did you get to know the app?
  - Flyer
  - Jazz meeting website
  - Project website
  - Friends
  - Other _____

③Privacy Protection Tools

- In this app, there was a tool that uses AI technology to erase people and "things that may contain privacy information" from the background photo you took. Did you use the privacy protection tool?
  - Used it
  - Did not use it →④Please flip over to proceed on to the "other".
- How was the privacy protection tool?
  - Very useful
  - Useful
  - Neither
  - Useless
  - Totally useless

Figure 44. Pilot4 questionnaire part I



③Privacy Protection Tools

- Did the privacy protection tool appropriately erase the parts of the photo that "might contain privacy information" such as people in the photo?
  - ○ Erased very appropriately
  - ○ Erased appropriately
  - ○ Neither
  - ○ Not erased appropriately
  - ○ Not erased appropriately at all

④Other

- What is your gender?
  - ○ Women
  - ○ Men
  - ○ Other
  - ○ Make no reply
- What is your age group?
  - ○ Under 12 years old
  - ○ 13～19 years old
  - ○ 20～39 years old
  - ○ 40～59 years old
  - ○ 60～79 years old
  - ○ Over 80 years old
- Do you live in Fujisawa?
  - ○ Yes
  - ○ No(Japan)
  - ○ No(Abroad)
  - ○ Make no reply

- Please fill in if there are any feedback form the event.

Figure 45. Pilot4 questionnaire part II

The main results are as below:

- Regarding Shonan Fujisawa Jazz Meeting event, two questions were evaluated:
  - Out of 20 answers obtained, 35% were quite satisfied with the event while 60% were very satisfied, as can be seen in the following figure.

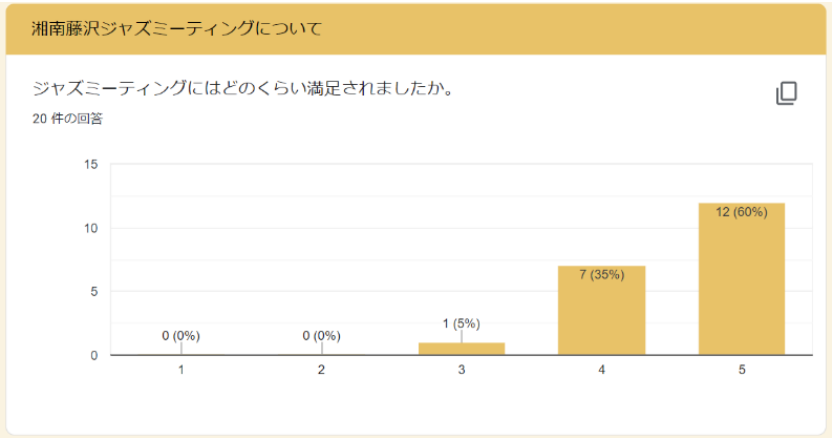


Figure 46. Q1: How satisfied were you with the Jazz Meeting?

- 14 users provided the names of the artists that they would like listen to again.

Figure 47. Q2: Are there any particular bands you would like to listen to again?

- Regarding SmileCityReport app, five questions were included:
  - Out of 20 answers obtained, all of them were satisfied with the SmileCityReport app: 40% were quite and 40% were very satisfied, as can be seen in the next figure.

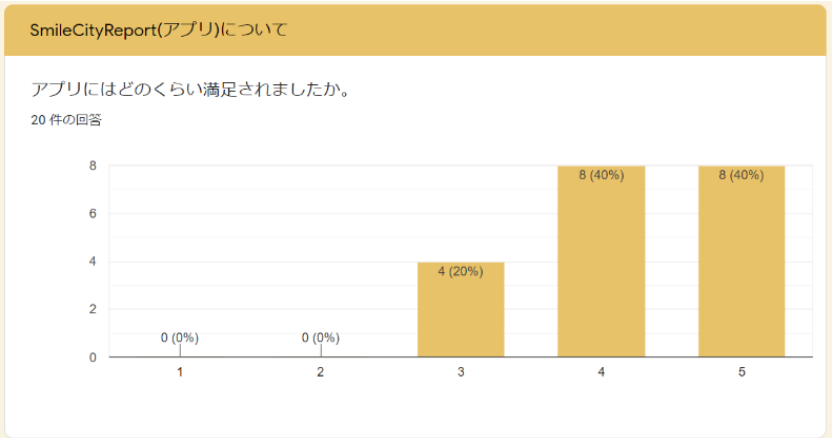


Figure 48. Q3: How satisfied were you with the app?

- Out of 20 answers obtained, all of them considered that posts were useful, as can be seen in the next figure.

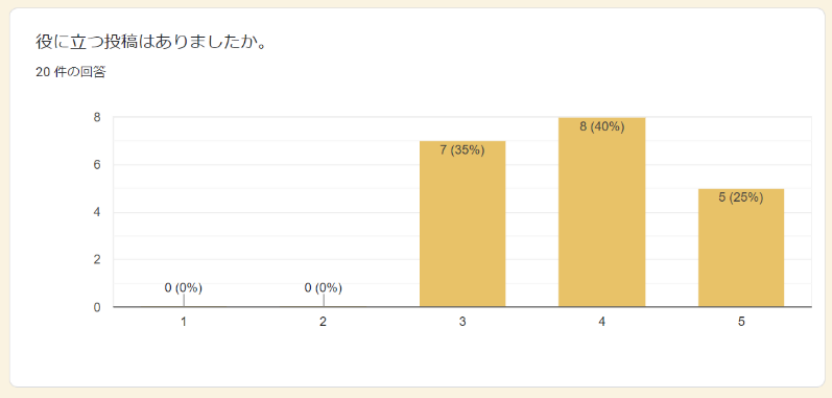


Figure 49. Q4: Were there any useful posts?

- Out of 17 answers obtained, more than 58% would like to use this app.

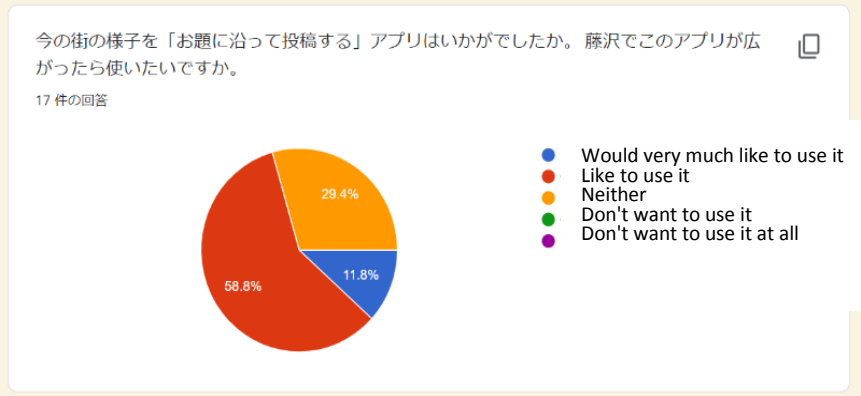


Figure 50. Q5: How did you like to use the SCR app?

- Out of 17 answers obtained, more than 40% considered interesting the ability to take pictures of yourself and the scenery at the same, while other 40% considered it very interesting.

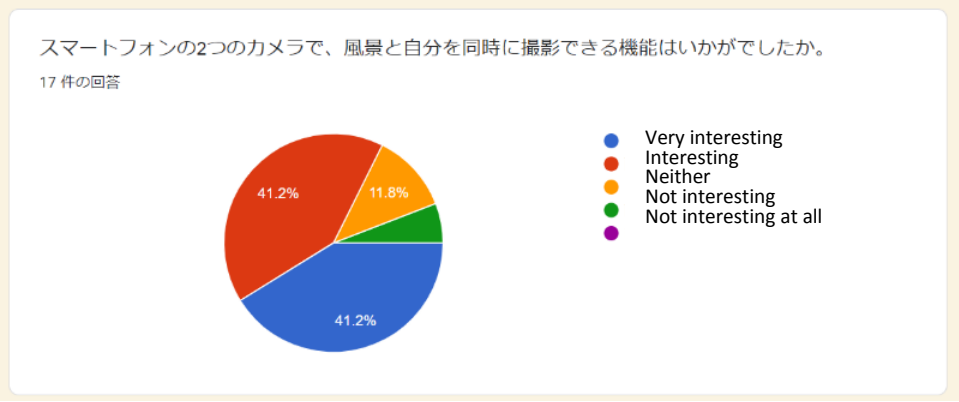


Figure 51. Q6: How about the ability to take pictures using the two cameras of your smartphone?

- Out of 20 answers obtained, 65% got to know the app through a Flyer while 20% did it through the Jazz meeting website.

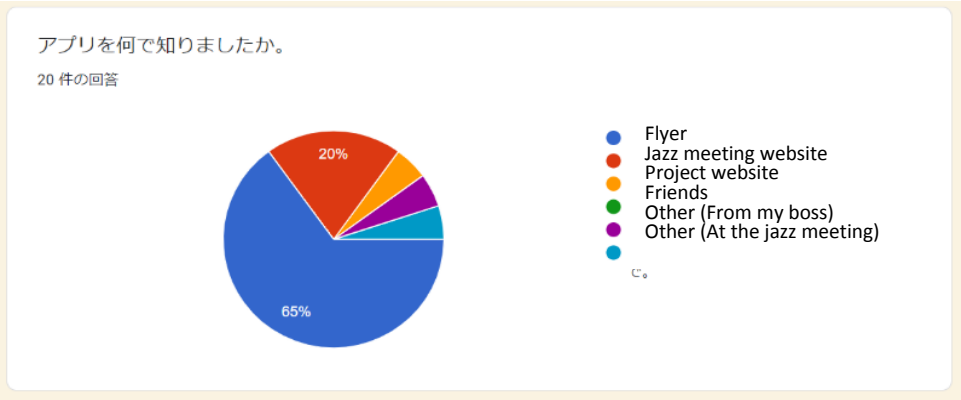


Figure 52. Q7: How did you get to know the app?

- Regarding privacy protection tools, three issues were raised:
  - Out of 17 answers obtained, more than 76 % did not use the tool which allows to erase people and "things that may contain privacy information" from the background photo you took.

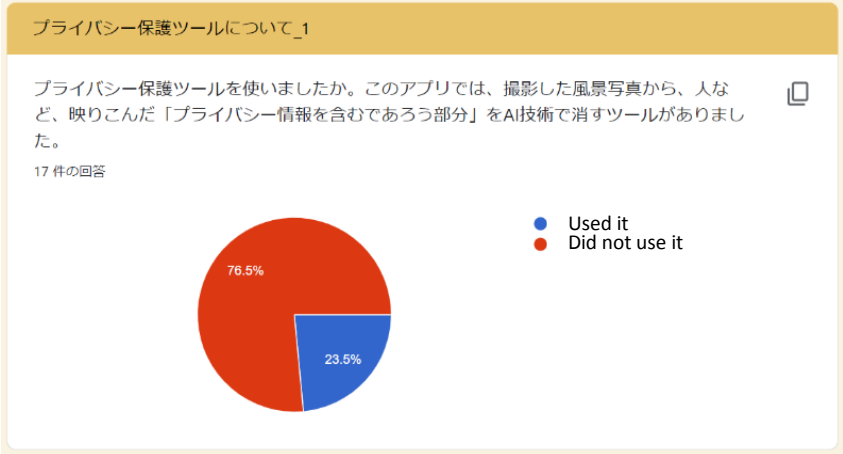


Figure 53. Q8: Did you use the privacy protection tool?

  - Out of the 7 participants, 43% considered useful the privacy protection tool.

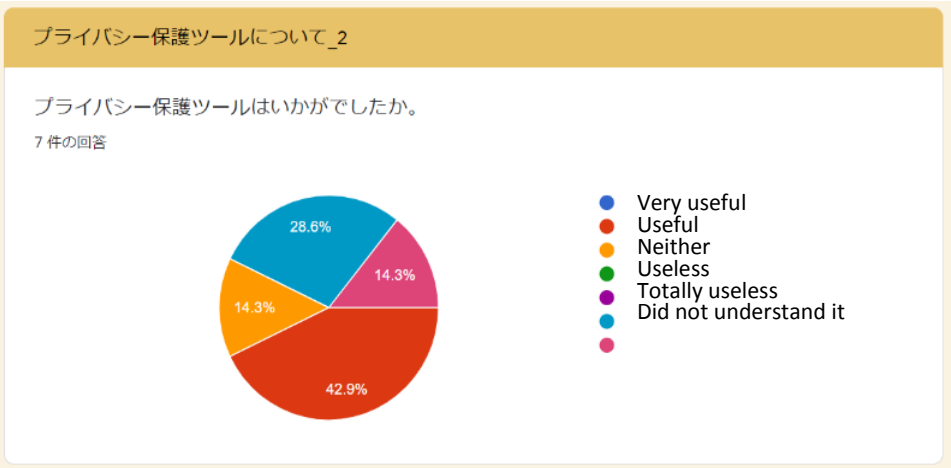


Figure 54. Q9: How was the privacy protection tool?

- Out of the 4 answers obtained, 50% considered that the privacy protection tool worked as expected, appropriately erasing the parts of the photo that “might contain privacy information”.

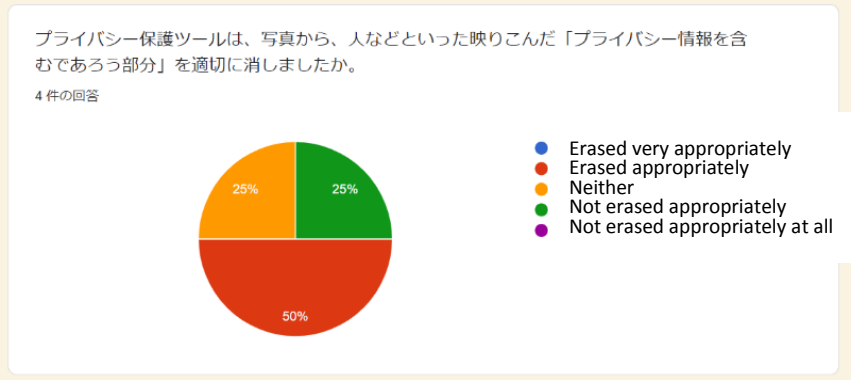


Figure 55. Q10: Did the privacy protection tool work as expected?

- Finally, other questions section includes more general questions related to gender and range of age of participants. Out of the 20 participants, 45% were women while 40% were men; while in terms of age, 55% of the participants belonged to 40-59 age group, 25% of them were in the 20-39 age group, as can be seen in the following figures.

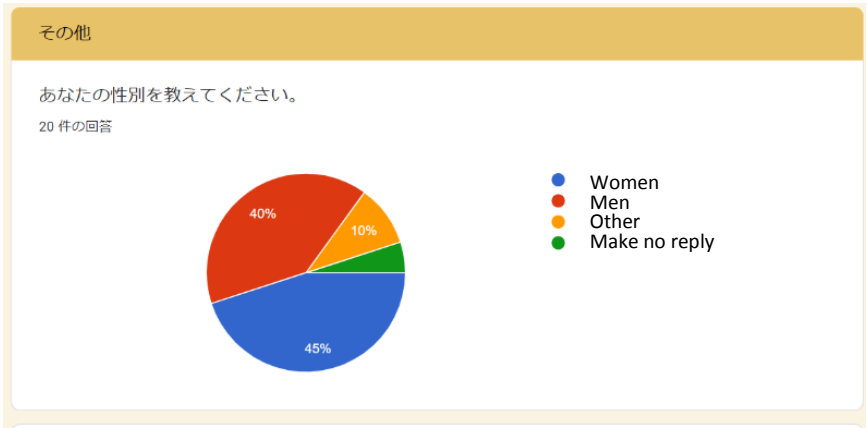


Figure 56. Q11: What is your gender?

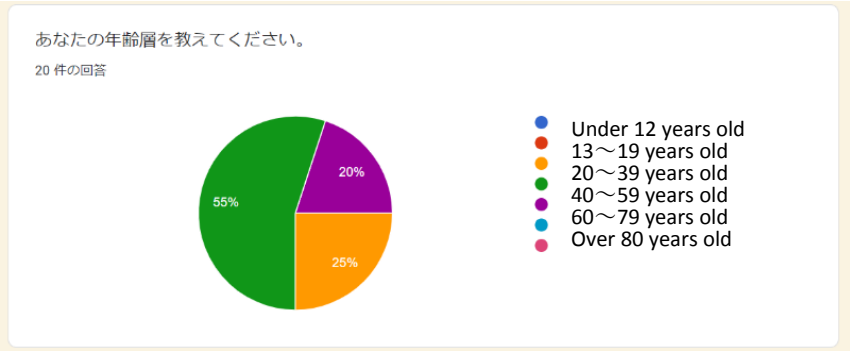


Figure 57. Q12: What is your age group?