



Multi-layered Security Technologies

for hyper-connected
smart cities

D2.1: M-Sec use cases description

January 2019



Grant Agreement No. 814917

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

Project acronym	M-Sec
Deliverable	D2.1 M-Sec use cases description
Work Package	WP2
Submission date	January 2019
Deliverable lead	Arturo Medela (TST) / Jin Nakasawa (KEIO)
Authors	Arturo Medela (TST), Vanessa Clemente, Tomás García (WLI), Sonia Sotero (AYTOSAN), Jin Nakasawa (KEIO), Keiko Doguchi (NTTE)
Internal reviewer	Vanessa Clemente, Tomás García (WLI) / Rui Tanabe, Aamir Bokhari (YNU)
Dissemination Level	Public
Type of deliverable	R

Worldline



TST



NTTEAST



YNU

大学共同利用機関法人 情報・システム研究機構
国立情報学研究所
National Institute of Informatics



NTT DATA
Trusted Global Innovator



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

- V0.1, 20/September/2018, Arturo Medela, Content, Full ToC
- V0.2, 24/October/2018, Arturo Medela, ToC updated, Reviewed
- V0.3, 25/October/2018, Arturo Medela, ToC updated
- V0.4, 30/October/2018, Jin Nakasawa, Use Case 3 description
- V0.5, 08/November/2018, Arturo Medela, Contributions to sections 1-3
- V0.6, 09/November/2018, Jin Nakasawa, Use Case 4 description
- V0.7, 13/November/2018, Vanessa Clemente, Use Case 2 description
- V0.8, 16/November/2018, Arturo Medela, Use Cases 1 & 6 description
- V0.9, 19/November/2018, Keiko Doguchi, Use Case 5 description
- v1.0, 22/November/2018, Arturo Medela, Annexes 1 & 2
- v1.1, 30/November/2018, Jin Nakasawa, Annexes 3 & 4
- v1.2, 30/November/2018, Arturo Medela, Update on Section 3, Surveys for Use Cases 1 & 6
- v1.3, 4/December/2018, Tomás García, Use Case 2 description
- v1.4, 5/December/2018, Vanessa Clemente, Use Case 2 description review & English survey Use Case 2
- v1.5, 7/December/2018, Arturo Medela, General contributions and editorial issues fixed
- v1.6, 10/December/2018, Vanessa Clemente, Descriptive template Use Case 2
- v1.7, 11/December/2018, Arturo Medela & Sonia Sotero, Use Case 1 Info and UC 1&6 survey results
- v1.8, 13/December/2018, Sonia Sotero, incorporation of UC 2 survey results
- v1.9, 14/December/2018, Vanessa Clemente, final conclusions of survey results within Use Case 2
- v1.10, 14/December/2018, Sonia Sotero, survey clarifications within UC 2
- v2.0, 14/December/2018, Arturo Medela, clean version ready for internal review
- v2.1, 18/December/2018, Vanessa Clemente & Tomás García, added comments after reviewing the document
- v2.2/2.3, 19/December/2018, Jin Nakasawa, Arturo Medela, response to internal review comments
- v2.4/2.5, 20/December/2018, Keiko Doguchi, Arturo Medela, response to internal review comments
- v2.6, 10/January/2018, YNU, review
- v2.7, 11/January/2018, NTTE, KEIO, updates and answer to comments
- v2.8, 11/January/2018, TST and F6S, merge contributions and clean report
- v2.9, 16/January/2019, Vanessa Clemente, suppression of pilot 2.3 within Use Case 2
- v3.1, 21/January/2019, KEIO, updates on use cases 3 & 4
- v3.2, 22/January/2019, TST and AYTOSAN, answer to remaining comments
- v3.3, 23/January/2019, KEIO, survey results
- v3.4, 23/January/2019, TST, report ready for final internal review
- v3.5, 24/January/2019, YNU, review
- v3.6, 28/January/2019, WLI review
- v3.7, 31/January/2019, TST, KEIO, NTTE, AYTOSAN, resolution of comments





Table of Contents

Table of Contents	4
List of Tables	6
List of Figures.....	7
Glossary	9
References.....	10
1. Introduction	11
1.1 Relation to other WPs and Tasks.....	11
1.2 Methodology followed	11
2. M-Sec at a glimpse.....	13
2.1 What is M-Sec?	13
2.2 State of the Art	13
2.3 M-Sec use cases: an initial approach.....	14
2.4 Relevant Stakeholders	15
3. Means to describe Use Cases	16
3.1 Descriptive Template.....	16
3.2 Gathering stakeholder's views	24
4. Use Cases	25
4.1 Santander Use Cases	25
Use Case 1: Reliable IoT devices with multi-layered security for a smart city	26
Use Case 2: Home Monitoring & Wellbeing Tele-assistance for active and independent ageing people	30
4.2 Fujisawa Use Cases	40
Use case 3: Secure and Trustworthy Urban Environment Monitoring with Automotive, Participatory, and Virtual Sensing Techniques.....	41
Use case 4: Secure and Trustworthy Hyper-connected Citizen Care	46
4.3 Cross-border Use Cases	49
Use Case 5: A marketplace of IoT services for effective decision making.....	49
Use Case 6: Citizens as sensor	53
5. Conclusions	57





Annex 1 – Use Case Surveys	58
Use Case 1 Survey	58
Use Case 2 Survey	63
Use Cases 3, 4 & 5 Surveys (originally in Japanese).....	68
Use Case 6 Survey	74
Annex 2 – Stakeholders Surveys results	79



List of Tables

Table 1: Use Case 2 description of potential measurements.....	31
Table 2: Use Cases scenario covered, implementation and target users.....	32
Table 3: Use Cases context and set-up.....	33
Table 4: Use Case 2 interest and motivations	34
Table 5: Use case 2.1 Tele-assistance & emergencies features	35
Table 6: Use case 2.2 Social & Physical Wellbeing features	37
Table 7: Use Cases 2 security requirements.....	39
Table 8: Examples of Environmental Data Captured in Use case 3.....	41
Table 9: Use Cases 3 security requirements.....	45
Table 10: Use Cases 5 security requirements.....	52
Table 11: Devices owned by the participants.....	89



List of Figures

Figure 1: M-Sec – Requirements analysis methodology	12
Figure 2: M-Sec – Stakeholders value chain as basis for the requirements elicitation.....	15
Figure 3: M-Sec – Use Cases Scenarios general description	16
Figure 4: M-Sec – Use Case detailed description.....	17
Figure 5: M-Sec – Use Case 1 detailed description	18
Figure 6: M-Sec – Use Case 2 detailed description	19
Figure 7: M-Sec – Use Case 3 detailed description	20
Figure 8: M-Sec – Use Case 4 detailed description	21
Figure 9: M-Sec – Use Case 5 detailed description	22
Figure 10: M-Sec – Use Case 6 detailed description	23
Figure 11: A view of Santander	25
Figure 12: Use Case 1 UML diagram.....	28
Figure 13: Use Case 2 functionalities.....	31
Figure 14: Use case 2.1 Tele-assistance & emergencies UML diagram.....	36
Figure 15: Use Case 2.2 Social and Physical Wellbeing UML diagram	37
Figure 16: Aerial view of Fujisawa	40
Figure 17: Automotive Sensing Trucks in Fujisawa City	42
Figure 18: Use Case 3 UML Diagram	44
Figure 19: Use Case 4 UML diagram.....	47
Figure 20: Use Case 5 UML Diagram	51
Figure 21: Use Case 6 UML diagram.....	54
Figure 22: Use Case 1 Survey Introduction.....	58
Figure 23: Use Case 1 Survey Step 1.....	59
Figure 24: Use Case 1 Survey Step 2.....	60
Figure 25: Use Case 1 Survey Step 3.....	61
Figure 26: Use Case 1 Survey Step 4.....	62
Figure 27: Use Case 6 Survey Introduction.....	74
Figure 28: Use Case 6 Survey Step 1.....	75



Figure 29: Use Case 6 Survey Step 2.....	76
Figure 30: Use Case 6 Survey Step 3.....	77
Figure 31: Use Case 6 Survey Step 4.....	78
Figure 32: Survey – Participant profile	79
Figure 33: Survey - Technology and devices.....	80
Figure 34: Survey - Threats and willingness	80
Figure 35: Survey - Previous participations	81
Figure 36: Telecare Survey – Participant profile	81
Figure 37: Telecare Survey – Technology and devices	82
Figure 38: Telecare Survey – Security & privacy	83
Figure 39: Telecare Survey – Evaluating features	84
Figure 40: Civic centres Survey – Participant profile	84
Figure 41: Civic centres Survey – Technology and devices.....	85
Figure 42: Civic centres Survey – Security & Privacy	86
Figure 43: Civic centres Survey – Evaluating features	86
Figure 44: Survey – Participants profile (Use Cases 3, 4, 5)	87
Figure 45: Survey – Participants Experience (above) and Attitude (below) to Information Technology.....	88
Figure 46: Survey – Threats in Use of Information Technology	90
Figure 47: Survey – If all of the threats mentioned above are resolved, would you like to utilize environmental measurements in regional IoT (to introduce it as a local government, to utilize data as a citizen or company for daily life etc)?	90
Figure 48: Survey – If all of the threats mentioned above are resolved, would you like to utilize "securely-collected data on the local area and people" in regional IoT (to introduce it as a local government, to utilize data as a citizen or company for daily life etc)?	91



Glossary

API	Application Programming Interface
CO ₂	Carbon Dioxide
CPS	Cyber-Physical Systems
DTMF	Dual-Tone Multi-Frequency
EDPB	European Data Protection Board
FIRE	Future Internet Research and Experimentation
GDPR	General Data Protection Regulation
ICT	Information and Communication Technologies
IoT	Internet of Things
KPI	Key Performance Indicator
PD	Personal Data
PIPA	Personal Information Protection Act
QoL	Quality of Life
SLA	Service Level Agreement
SME	Small Medium Enterprise
SMS	Short Message Service
UC	Use Case
UML	Unified Modelling Language





References

- [AIA] Apiumhub, “Artificial Intelligence – In Math I trust”, <https://apiumhub.com/tech-blog-barcelona/artificial-intelligence/>
- [ARM] ARMOUR project, <https://www.armour-project.eu/about/>
- [BRA] Brain-IoT (*model-Based fRamework for dependable sensing and Actuation in iNtelligent decentralized IoT systems*), <http://www.brain-iot.eu/>
- [BIG] BIG IoT (*Bridging the Interoperability Gap of the Internet of Things*), <http://big-iot.eu/>
- [CYB] Apiumhub, “Little known ways to prevent Internet Frauds”, <https://apiumhub.com/tech-blog-barcelona/ways-prevent-internet-frauds/>
- [D22] Deliverable 2.2 “M-Sec pilots definition, setup and citizen involvement plan”, M-Sec project, Month 8 (February 2019)
- [D511] Deliverable 5.11, “M-Sec GDPR compliance assessment report”, M-Sec project, Month 24 (June 2020)
- [MIR] CSO, “The Mirai botnet explained: How teen scammers and CCTV cameras almost brought down the internet”, <https://www.csoonline.com/article/3258748/security/the-mirai-botnet-explained-how-teen-scammers-and-cctv-cameras-almost-brought-down-the-internet.htm>
- [RER] RERUM Project (*REliable, Resilient and secUre IoT for sMart city applications*), <https://ict-rerum.eu/>





1. Introduction

This document provides the initial version of M-Sec reference use cases, requirements and technical reference architecture. In detail, it presents the use cases that will be studied and implemented during the project, the requirements that stem from them, and the M-Sec technical architecture, including the binding between its logical modules and the technological assets that can be adopted for its implementation.

The different reference use cases are described adopting a common approach: for each of them a brief description of the use case, involved stakeholders, UML diagrams, and a summary of the main requirements considered in each one of them; in addition, faced Big Data challenges, and its replication potentiality are reported.

Finally, conclusions are reported in section 5, paving the way forward for the next stage of the project.

1.1 Relation to other WPs and Tasks

Relationship to other tasks: T2.1 will provide initial insight into the characteristics, goals and ambitions of every use case paving the way for T2.2 to define thoroughly the pilots that will be deployed to demonstrate them all, and sketching the methods to proceed with the overall integration in T2.3. It will also help defining to some extent the M-Sec architecture that will be the duty of T3.2, and will contribute to feed the list of potential risks that T3.3 will create.

1.2 Methodology followed

The analysis starts with a definition of the M-Sec concept, including an overview of the use cases, use case diagrams (described through UML diagrams) and the stakeholders involved, allowing the reader to understand the context of the project and the role of the various stakeholders. In addition, a recap of potential impact of each use case over the current regulation in both Europe, with the GDPR (*General Data Protection Regulation*), and Japan, with the PIPA (*Personal Information Protection Act*) is addressed. As a next step, the consortium partners give an overview of the technologies that are going to be involved in the project and the perspective of using them in order to implement the M-Sec concept.

Similar projects and corresponding background are also mentioned in order to identify the state-of-the-art and the previous achievements that can be used as a starting point. Furthermore, a brief and simple listing of potentially interesting requirements can be offered in certain use cases. These requirements will in the end act as a reference for the design, implementation and validation phases of the project. Figure 1 gives an overview of the methodology that will be followed.

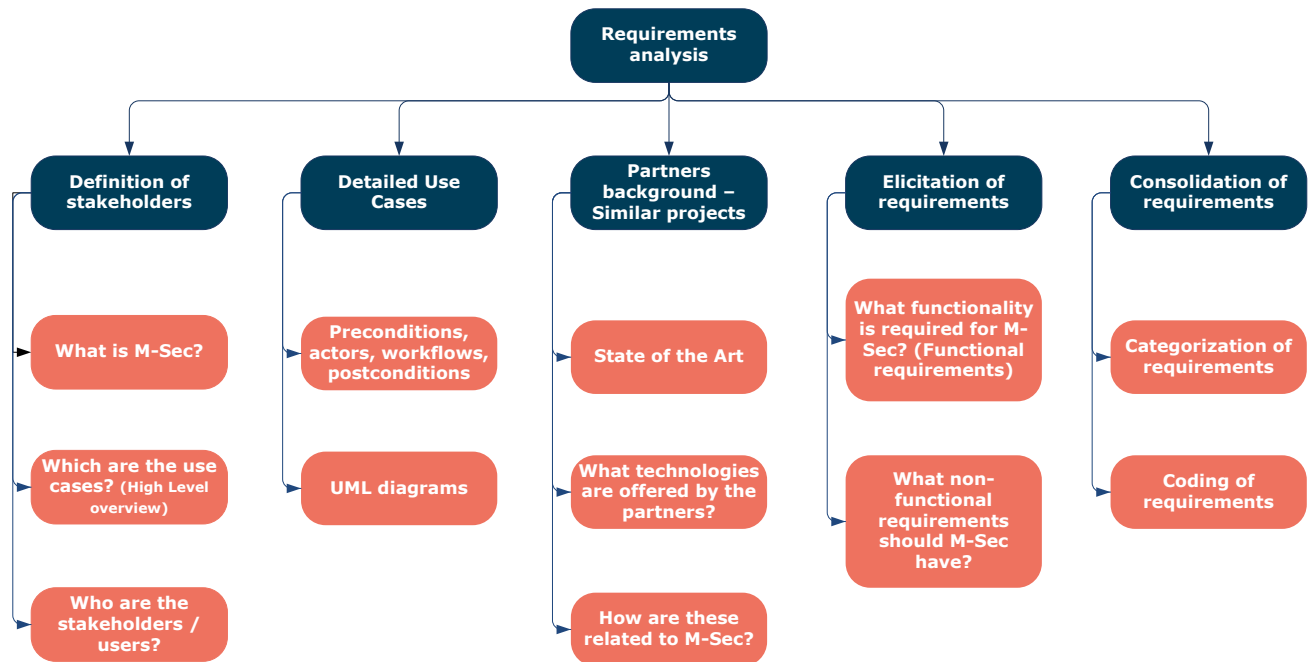


Figure 1: M-Sec – Requirements analysis methodology

A complete listing and description of the M-Sec functional requirements will be depicted in Work Package 3 deliverables, starting with D3.1 in Month 8 and being refined in D3.2 in Month 24.



2. M-Sec at a glimpse

2.1 What is M-Sec?

Currently, state-of-the-art IoT (Internet of Things) systems in smart cities rely on architectures which promote a centralized data collection and processing approach, which introduces several limitations both in terms of the supported applications and in terms of the business models that they enable. In particular, smart city platforms are mainly centralized IoT/Cloud infrastructures and thus they tend to be:

- Inefficient in handling actuation such as use cases involving invocation and control over sensors and physical devices.
- Prone to “complete failures” since they dispose with centralized control by a limited number of administrative entities (e.g., service providers, smart cities, service operators).
- Inflexible in the incorporation of innovative applications and new business models, mainly because they require heavy administration and do not facilitate peer-to-peer decentralized interactions between people and “things”.

Moreover, in modern smart city applications there is an emerging need of end-to-end security since many data sources may contain sensitive information that raises issue on privacy and data protection.

Therefore, there is room for improvement in these topics and taking that as a starting point the main goal of M-Sec project is to research, develop, deploy and demonstrate Multi-layered Security technologies to ensure hyper connected smart cities and empower IoT stakeholders with an innovative platform which leverages Blockchain, Big Data, Cloud and IoT security, upon which they can build innovative smart city applications. The project will explore secure, interoperable interactions between IoT elements based on a holistic secured cloud/edge/IoT context within a future smart city. Overall, the M-Sec paradigm will complement mainstream IoT/cloud technologies, through enabling the introduction and implementation of specific classes of applications and services, which are not efficiently supported by state-of-the-art architectures.

2.2 State of the Art

During recent years the European Commission included the Security and Privacy in IoT topic as part of the ambitious IoT Strategy in Horizon 2020. Under this topic, there is an interest in addressing security, trust and privacy in IoT platforms, services and applications. A particular emphasis is on Blockchain and Distributed Ledger technology as an enabler.

Several projects have been funded under this scope. One of them, even previous to this program, is the RERUM Project (*REliable, Resilient and secUre IoT for sMart city applications*) [RER], which ran from 2013 to 2016. RERUM aimed to develop, evaluate, and trial an architectural framework for dependable, reliable, and secure networks of heterogeneous smart objects supporting innovative Smart City applications. The framework will be based on the concept of “security and privacy by design”, addressing the most critical factors for the success of Smart City applications.



The project BIG IoT (*Bridging the Interoperability Gap of the Internet of Things*) [BIG], ignites an IoT Ecosystem of services and applications. Starting with 8 IoT platforms from the BIG IoT partner companies the project will implement services and applications first for Barcelona, Piedmont, and Berlin/Wolfsburg. This way, BIG IoT will demonstrate interoperability in different Smart Cities.

ARMOUR project [ARM], aims to address Security and Trust issues on Internet of Things by providing duly tested, benchmarked and certified Security & Trust technological solutions for large-scale IoT using upgraded FIRE (*Future Internet Research and Experimentation*) large-scale IoT/Cloud test beds properly-equipped for Security & Trust experimentations. ARMOUR identified 3 goals that define the approach being used to achieve the proposed Security and Trust solutions:

- Enhance two outstanding FIRE testbeds with the ARMOUR experimentation toolbox for enabling large-scale IoT Security & Trust experiments;
- Deliver six properly experimented, suitably validated and duly benchmarked methods and technologies for enabling Security & Trust in the large-scale IoT;
- Define a framework to support the design of Secure & Trusted IoT applications as well as establishing a certification scheme for setting confidence on Security & Trust IoT solutions.

On the other hand, Brain-IoT (*model-Based fRamework for dependable sensing and Actuation in iNtelligent decentralized IoT systems*) [BRA], aims at establishing a framework and methodology that supports smart autonomous and cooperative behaviours of populations of heterogeneous IoT platforms that are also closely interacting with Cyber-Physical systems (CPS). Brain-IoT will employ highly dynamic federations of heterogeneous IoT platforms, mechanisms enforcing privacy and data ownership policies as well as open semantic models enabling interoperable operations and exchange of data and control features. Brain-IoT will also offer model-based tools easing the development of innovative, tightly integrated IoT and CPS solutions.

2.3 M-Sec use cases: an initial approach

M-Sec project brings together 6 Use Cases (UCs) provided by the 2 smart city partners involved and divided according to the following schema:

Use cases provided by Santander:

- SAN-UC1: Reliable IoT devices with multi-layered security for a smart city
- SAN-UC2: Home Monitoring & Wellbeing Tele-assistance for active and independent ageing people

Use cases provided by Fujisawa:

- FUJ-UC3: Secure and Trustworthy Urban Environment Monitoring with Automotive, Participatory, and Virtual Sensing Techniques
- FUJ-UC4: Secure and Trustworthy Hyper-connected Citizens Care

Use cases cross-border:

- CB-UC5: A marketplace of IoT services for effective decision making
- CB-UC6: Citizens as sensor



A detailed analysis of each one of these use cases is provided in section 4 of the current document.

2.4 Relevant Stakeholders

The project aims to get the involvement of the stakeholders in the whole value chain that the project brings. The following Figure 2 gives an overview of the M-Sec value chain.

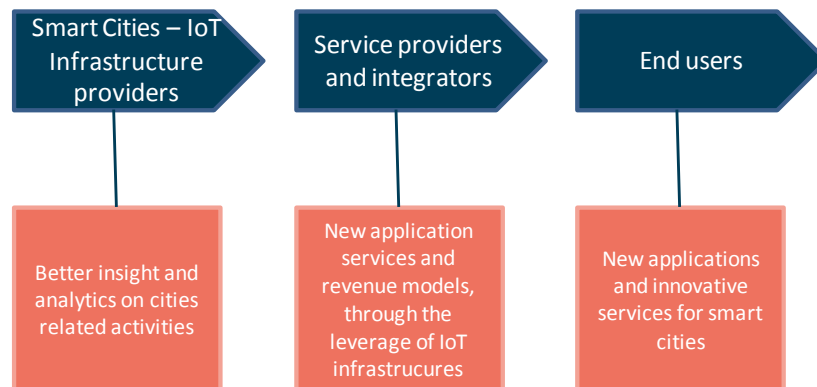


Figure 2: M-Sec – Stakeholders value chain as basis for the requirements elicitation

Note that M-Sec consortium includes all necessary stakeholders of the M-Sec value chain. In particular, the consortium includes smart city infrastructure providers (i.e. Santander and Fujisawa), technology providers as well as service providers and integrators (i.e. the technical partners from EU and JP side), end users as these are going to be recruited by the smart cities partners.

Smart Cities - IoT Infrastructure Providers: they provide their sensing infrastructure and the captured events to the M-Sec ecosystem. These providers will offer or lease their infrastructures in exchange of some cost/fee, or based on other participation incentive.

Service Providers and integrators: they will offer technology and application services over the infrastructures of one or more infrastructure providers. The service providers for instance can establish Service Level Agreements (SLAs) with infrastructure providers to offer B2B services on the basis of the M-Sec capabilities on big data analytics. Service providers will possibly endeavour to generate revenue streams based on subscriptions/fees of corporate end-users or individuals. The role of technology providers and integrators in the value chain is associated with the integration of the platform, as well as in the enhancement of the platform with new added value capabilities. Overall, integrators of M-Sec systems can use the software and/or middleware libraries of the project in order to build and deploy applications that leverage the M-Sec capabilities to offer added value services.

End Users: Consumers and individuals (including tourists) registering to the M-Sec services and consuming them mainly through smart phones. Individual users are less likely to employ subscription services, but they are likely to participate in the platform based on other forms of incentives (e.g. credits for using the platform as soon as they also contribute to the platform).



3. Means to describe Use Cases

The M-Sec consortium agreed on a strategy to fulfil the goal of achieving a complete and fully comprehensive description of every use case. Therefore, a template with a series of topics considered relevant must be completed by all partners in a joint effort, while also the stakeholder's perspective is taken into account through specific surveys. Both are properly presented in this section.

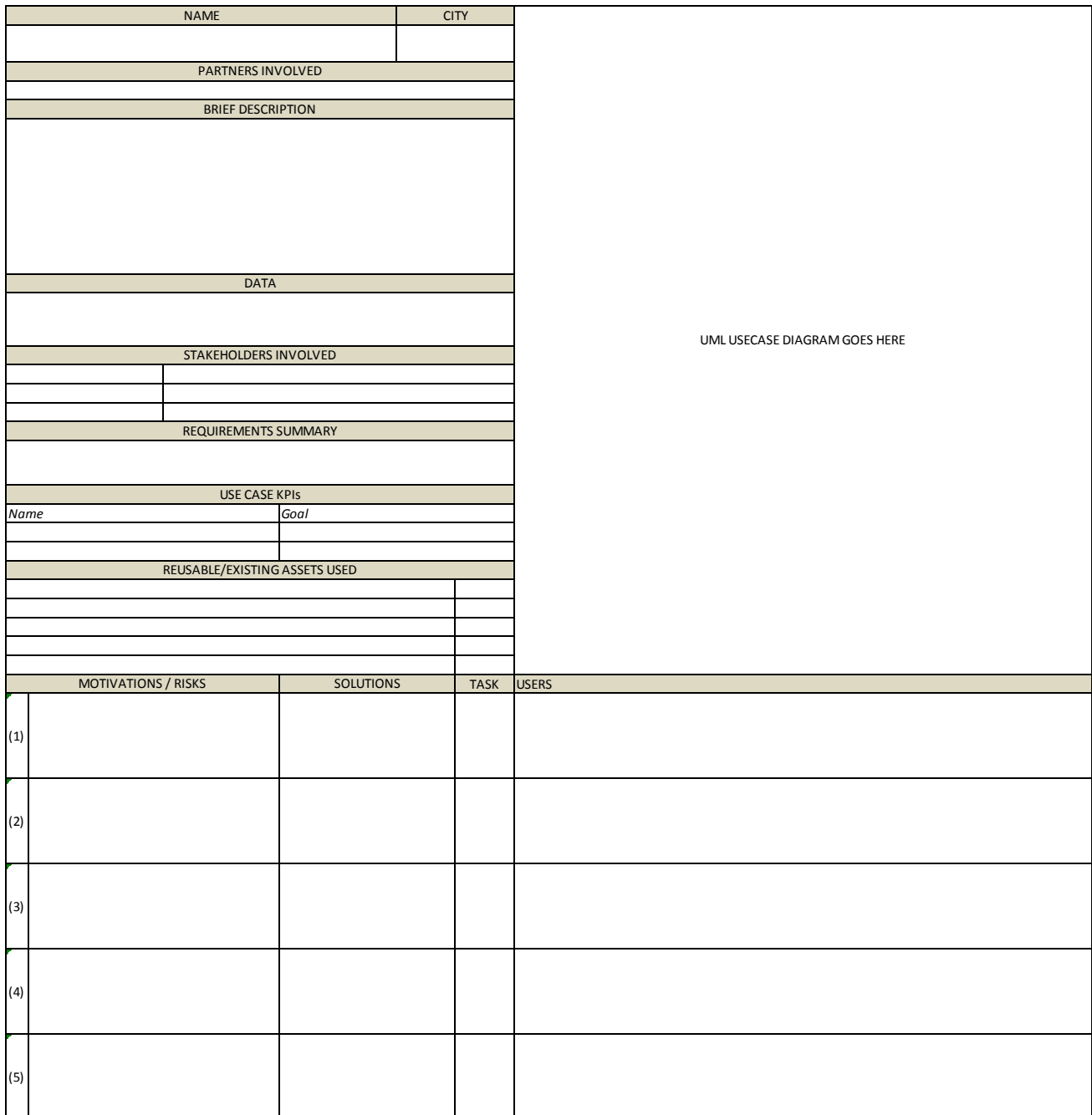
3.1 Descriptive Template

A first approach to this activity involves filling a table (shown in **¡Error! No se encuentra el origen de la referencia.**) where a general description of the use cases can be completed.

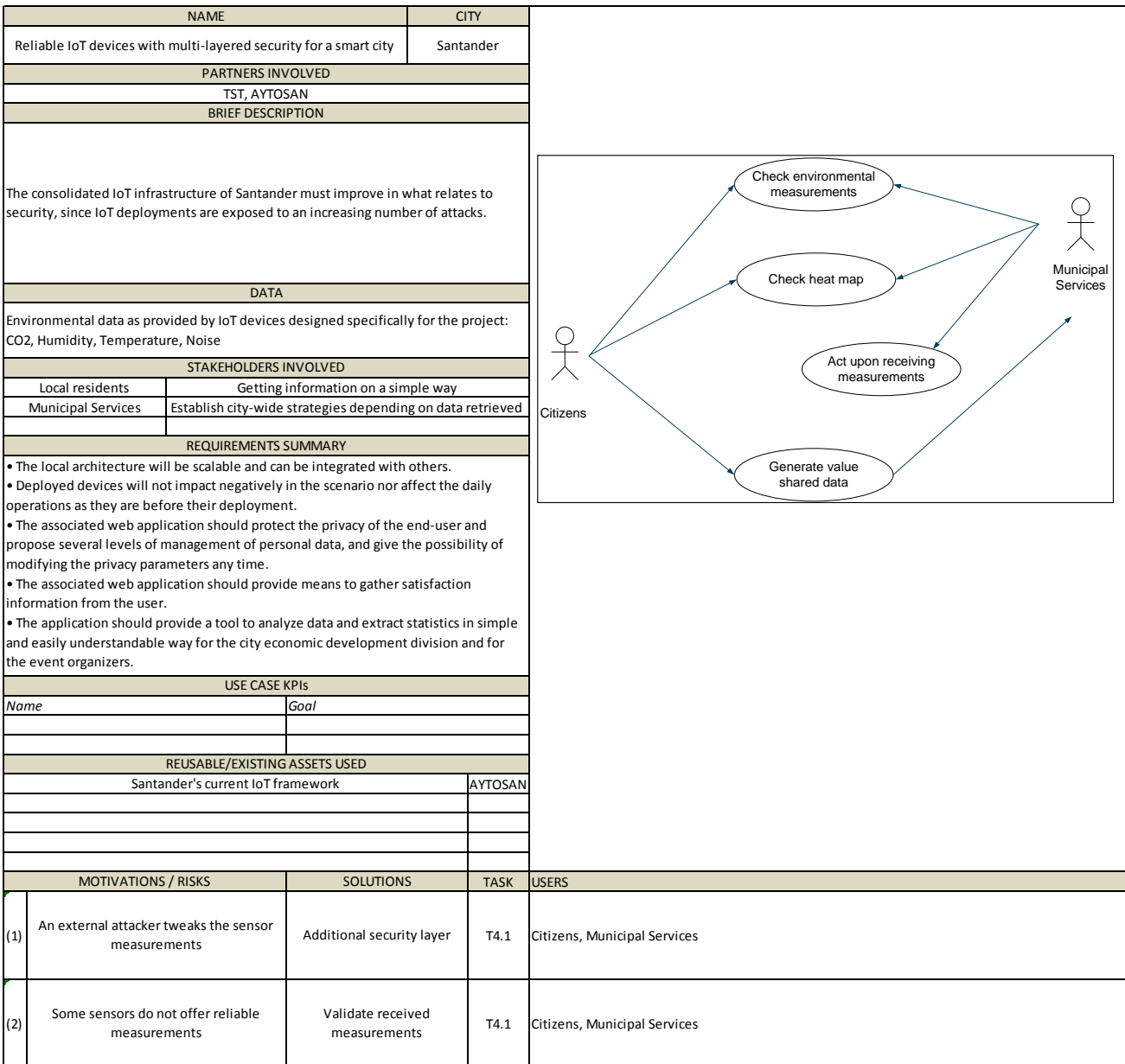
M-Sec Use Case Scenario									
		Pilot	Motivations / Needs	Solutions	Data	Target Users	Reusable / Existing Assets	Technology need to be added	Stakeholders
1	Reliable IoT devices with multi-layered security for a smart city	Santander							
2	Home Monitoring & Wellbeing Tele-assistance for active and independent ageing people	Santander							
3	Secure and Trustworthy Urban Environment Monitoring with Automotive, Participatory and Virtual Sensing Techniques	Fujisawa							
4	Secure and Trustworthy Hyper-connected Citizen Care	Fujisawa							
5	A marketplace of IoT services for effective decision making	EU-JP							
6	Citizens as sensor	EU-JP							

Figure 3: M-Sec – Use Cases Scenarios general description

The description of every use case will be based on a common template, highlighting various characteristics such as their innovative nature, impact on society, replicability, complementarity with other city use cases, difficulty of realization, etc. Figure 4 below depicts this template which helps to detail each use case features and characteristics.



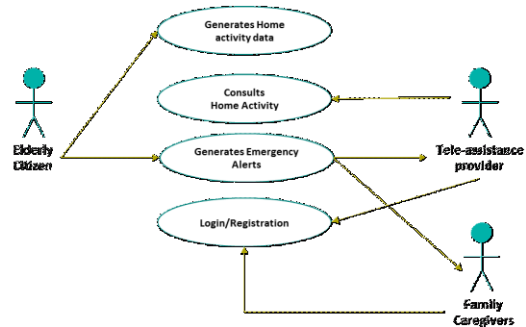
The consortium has worked in completing this template with the most relevant information related to each use case, which in turn served as the basis for the contents of this report. The following figures show the depiction of the shape the template took in every case.





NAME		CITY	
Home Monitoring & Wellbeing Tele-assistance for active and independent ageing people		Santander	
PARTNERS INVOLVED			
WUJ, AYIOSAN, TST			
BRIEF DESCRIPTION			
Worldline will use its Connected Assistance platform as a starting point, a solution that already covers some issues related with health and wellbeing. Additionally, a range of functionalities will be added in order to offer a complete solution not only on terms of wellbeing and health monitoring but also by making ageing people to feel safe at home through smart home sensors and less isolated through a video-call, chat tool so elderly people can stay longer and independently at their homes.			
DATA			
Health and wellbeing data			
STAKEHOLDERS INVOLVED			
Ageing people	As data producer and data consumer		
Relatives	As data consumer to get information about a family		
Caregivers	As data consumer to monitor patient's status		
Social Services / Tele-	As data consumer to monitor and track wellbeing and		
Dynamizer (City of Santander)	In some tasks within the pilots to promote and encourage participation of elders in the activities of the community		
REQUIREMENTS SUMMARY			
Data encryption			
Data access			
Access control			
Secure communication			
Multi-signature access			
REUSABLE/EXISTING ASSETS USED			
Santander's current monitoring system		AYIOSAN	
Connected Assistance platform		WUJ	
MOTIVATIONS / RISKS		SOLUTIONS	TASK
{1}	Target audience may involve oldest generations that have not adopted technology	Involve also relatives and caregivers will be involved with the aim that citizens can feel supported on the use of the application and all the IoT devices used.	T2.2
{2}	Security's concern	Create awareness about the benefits of the M-Sec platform not only when conducting the pilot, but also through dissemination and community activities.	T4.2 T4.4

Use case 2.1 Tele-assistance & emergencies UML diagram



Use Case 2.2 Social and Physical Wellbeing

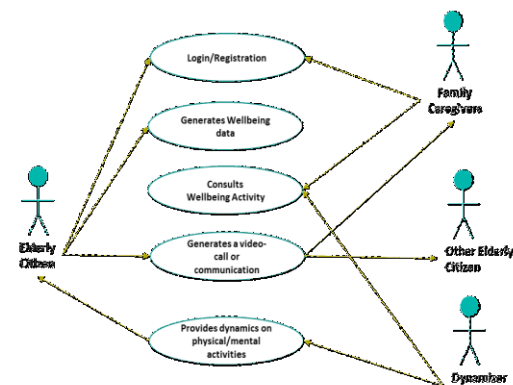


Figure 6: M-Sec – Use Case 2 detailed description



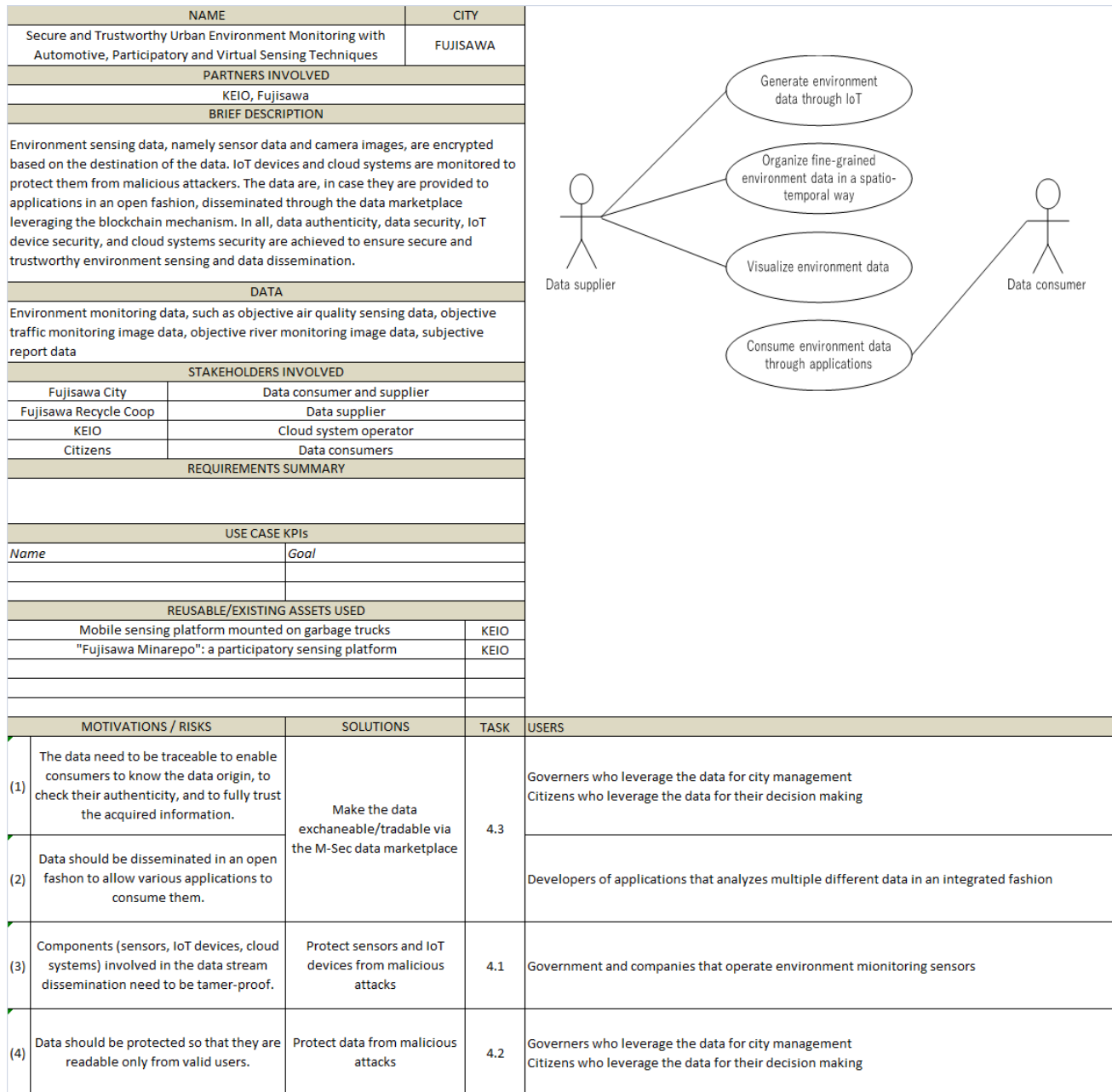
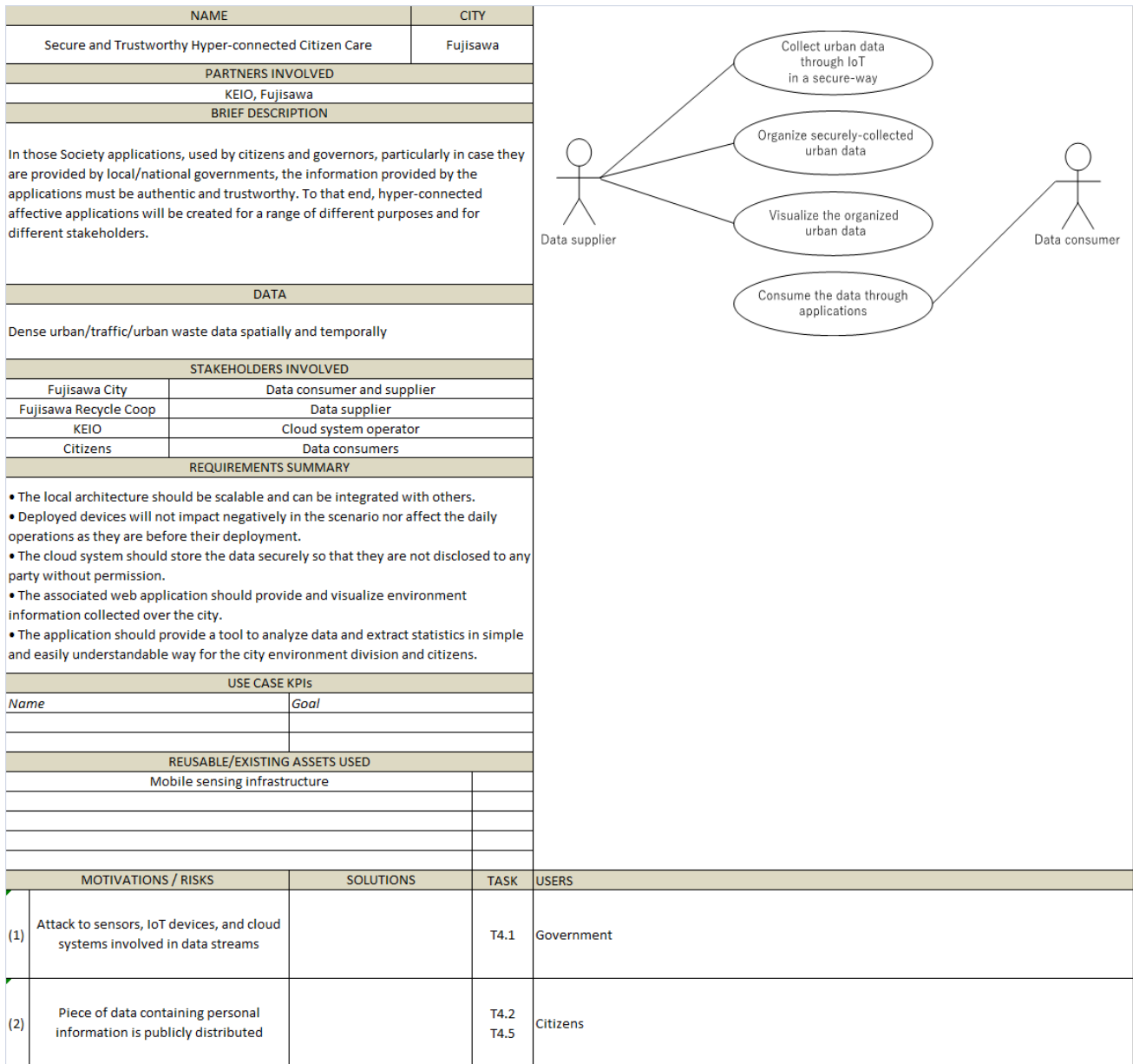


Figure 7: M-Sec – Use Case 3 detailed description



21



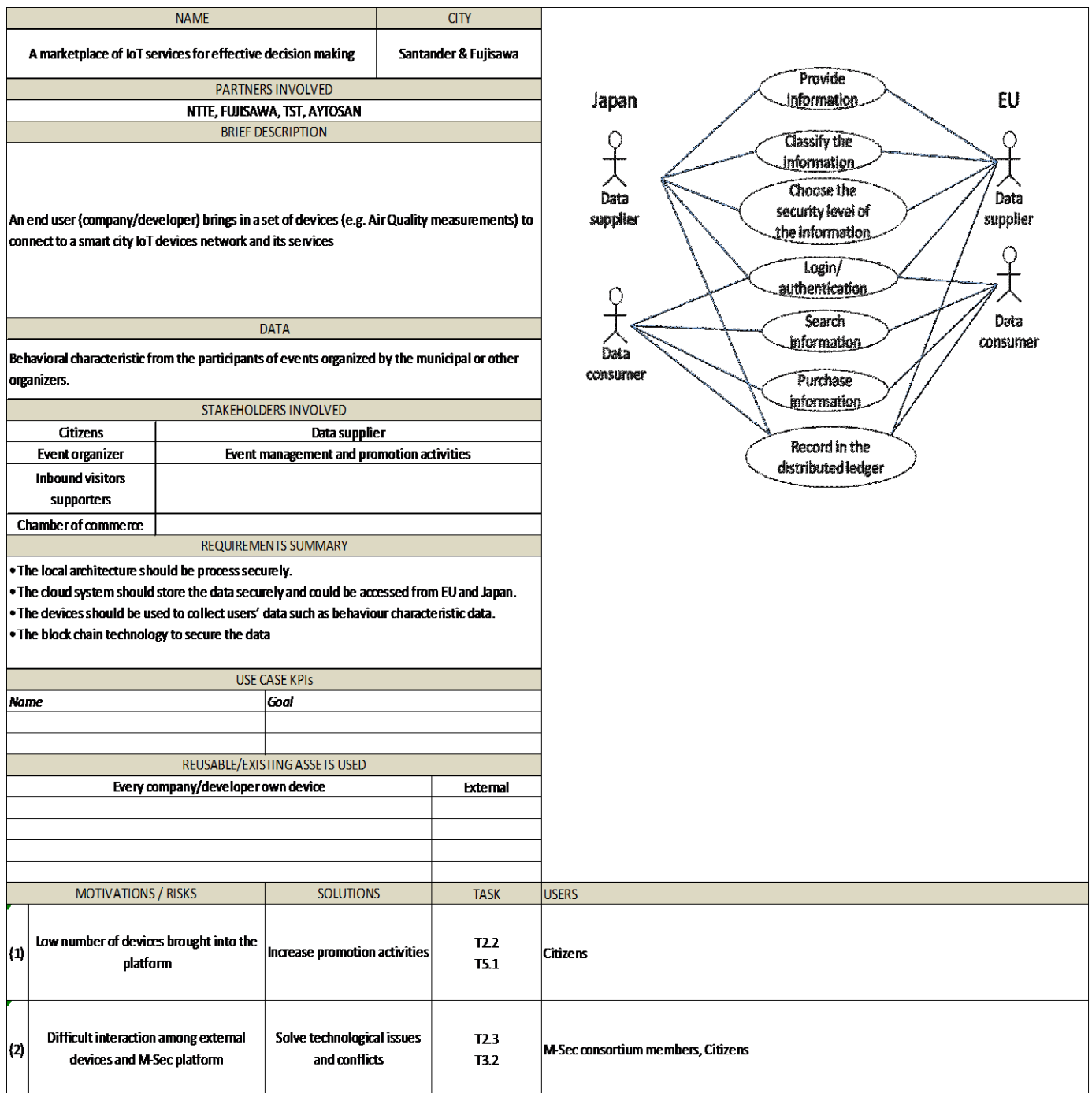


Figure 9: M-Sec – Use Case 5 detailed description

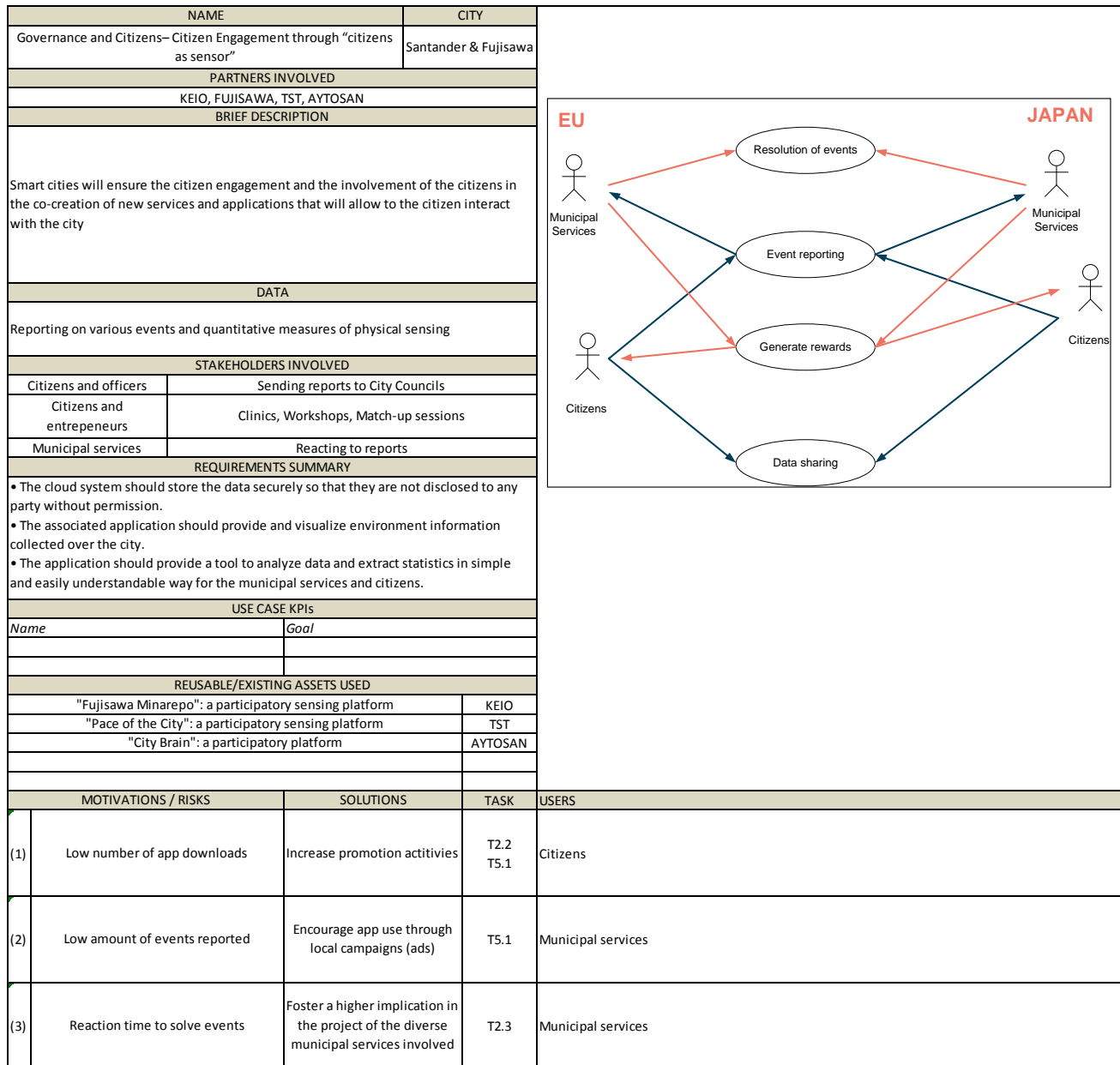


Figure 10: M-Sec – Use Case 6 detailed description



3.2 Gathering stakeholder's views

The second step will be to involve a wider set of stakeholders including citizens and entrepreneurs in the process of defining additional point of views for the use cases that are most important to them. To do so, partners in the consortium prepared some surveys which help to retrieve the general impressions and expectations they have when facing scenarios like the ones proposed by M-Sec.

These surveys were totally compliant with current personal data protection regulations, both in EU and Japan, since participant's contributions were totally anonymized. In some cases, they needed to provide an e-mail account, but no direct correlation between that e-mail address and the answers to the survey was established, nor any specific name and surname was asked for.

Each one of these surveys was suited to comply with the objectives pursued by each Use Case; therefore, apart from a set of common questions participants can find specific ones that contribute to better know what they expect and would like to use.

The results of the different surveys conducted during Q4 2018, which can be consulted in the Annex 2 of this report, help the consortium partners to extract useful learnings and tweak the initial ideas sketched for the pilots to conduct as part of the envisioned use cases, adding some features that participants have expressed a high interest in enjoying or avoiding those characteristics that receive a bad perception.



4. Use Cases

This section provides a detailed description of the updated use cases that are studied and implemented in the M-Sec Project.

4.1 Santander Use Cases

In recent years, the city of Santander (see Figure 11) has moved into the vanguard of smart cities, improving public services and developing policies oriented towards its citizens as well as stimulating a new business model of productivity in the city. Several years ago, the city government had the perception that a new economic model was needed. This model has to be based on the confluence of innovation and development, thus benefiting from some of the strengths of our City and Region. As a consequence, various players have taken an active role in this transformation, including among others, University of Cantabria, SMEs working in the ICT (*Information and Communication Technologies*) area and the support of the Bank of Santander.

All these ingredients gave the city the opportunity to participate in different initiatives related to smart cities. Among them, the SmartSantander project represented a watershed in the way of conceiving and organizing innovation in the city. Santander is well-known as a living lab, a unique test bed to experiment with new technologies, applications and services.

At the municipal level, innovation is conceived as transversal to other areas of governance, coordinating the incorporation of new technologies with municipal services, which leads to an improvement in the services.



Figure 11: A view of Santander



Making Santander's systems and services smarter saves costs and increases efficiencies, contributing to a more liveable city, while positioning it for a long-term economic growth.

Innovation in management and governance provides qualitative improvements to the public services. In this scenario, the adoption of ICT technologies allows citizens to take an active role, improving how their city works and stimulates a thriving, knowledge-driven economy.

Santander reinvents itself to enhance the quality of life of its citizens with facilities and new services in keeping with the new times. Looking to the future, the traditional, elegant city is also now a ground-breaking city which takes risks and innovates, which embraces technology to make life a little easier with more and better services based on an intelligent use of the IoT.

The Internet of Things is a technological breakthrough that is completely revolutionizing our daily life. More and more devices are connected to the Internet. Today we can collect, store, analyze and manage more data to provide more effective solutions from the management and massive analysis of data and artificial intelligence apps [AIA]. None of that would be possible if we didn't have IoT devices to facilitate data gathering and collection. However, this scenario is also very attractive to cybercriminals [CYB], who see in the proliferation of devices and applications a great incentive for their activities. Therefore, the ground is ripe for an initiative like the one posed by M-Sec project to enter this ecosystem. Santander citizens will feel more confident and progress in their use of Smart City services the moment they rest assure them all are properly secured.

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

Description

The use case will deploy a series of novel IoT devices in selected locations in the city to both retrieve interesting environmental data along with a measurement of noise level while on the other hand will also be capable of sketching crowd heat maps, using as a source of information the number of mobile phones in the area.

Users will be able to check this data getting access to a public webpage which presents the values provided by the sensors deployed and offers them the option to rate how good they value that information. In addition, a system of providing rewards to the more active users will be evaluated to implement it in the latter stages of the piloting.

Therefore, the technological developments will focus on the creation of novel IoT devices which implement these kinds of features through the integration of different sensors while at the same time incorporate novel security layers, both from the hardware and the software standpoint, increasing their reliability and trustworthiness.

Interest

This Use Case implies a step in the *smartization* of the whole city and the involvement of citizens in the Municipality daily routines, as well as contributes to the generation of new datasets which may be used by entrepreneurs to develop new services or solutions, reinforcing the local ecosystem.





To refine the scope of this use case, the results of the survey conducted in Santander (see Annex 2) will be decisive, allowing the consortium to distinguish what the preferences of the citizens are and trying to put emphasis on developing solutions that satisfy their requests.

Stakeholders involved and means of interaction/engagement

The following stakeholders have been identified for the specific use case:

- Santander Smart City: acting as the IoT infrastructure provider where the use case will take place.
- Citizens: being the end user and getting information on a simple way valid for them to know whether, for instance, it is the proper time to go to a certain beach or not (perhaps according to the heat map it is too crowded). In addition, checking environmental measurements and/or noise levels they could even interact through certain means (e.g. scanning QR codes located in those spots that get them to a certain webpage) with municipal services whenever necessary to notify them something is wrong or weird.
- Municipal Services: exerting as service providers they could establish city-wide strategies depending on data retrieved from the heat maps (e.g. when is the best time to trigger a marketing initiative) and also act whenever the noise levels in certain spot increase dramatically.
- SMEs in the M-Sec consortium: considered as service providers and integrators, looking for novel ways to create a business model based on its IoT background and expertise and the novel applications developed for this environment.

The majority of these actors have already been contacted concerning the M-Sec project to introduce it and retrieve some initial informal opinions. In the following months, at least one physical meeting per stakeholder will be organized with the participation of the Santander Municipality and TST. A clear interest in the results of the project has been identified so far, since the results of this use case could derive in an improvement over the way citizens interact with the IoT devices deployed in the city and on how fast the Municipal Services act upon receiving a notification. As a conclusion of those meetings, it seems promising that through the execution of the pilots related to this Use Case, new and reliable city data sources will be available, including the new layers of security developed within M-Sec project. These data sources will be useful not only for municipal services and citizens, but will also be available to entrepreneurs.



Use Case Diagram

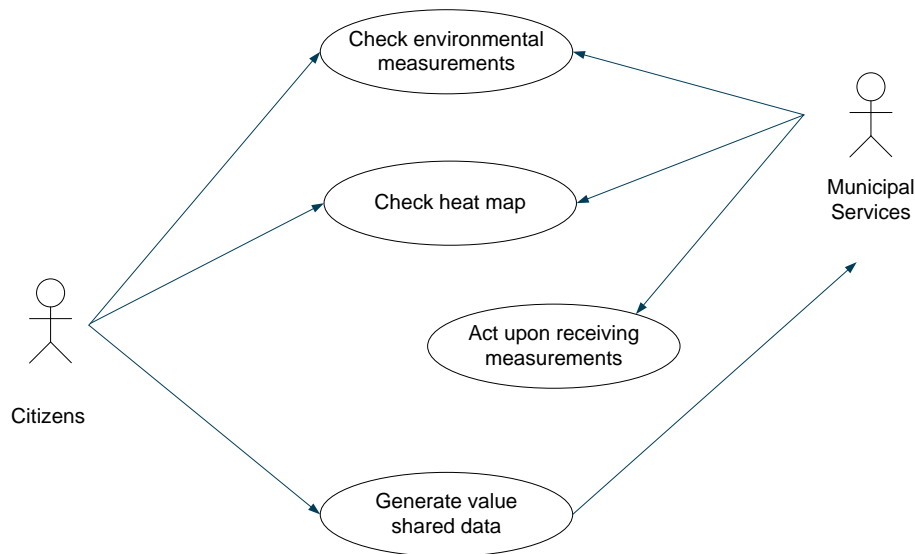


Figure 12: Use Case 1 UML diagram

Threats and Difficulty of realization

A potential threat to this particular use case could be related to the external tweaks produced over sensor measurements which derive in false reports related to the environmental measurements, going from irregular temperature and humidity readings to unusual noise level values (e.g. it is too high, so a special action is required) which could be tweaked by an attacker willing to trick the local administration into devoting more attention to certain areas of the city that don't really need it as much as others. Something similar can happen when sketching the crowd heat maps, due to the fact that the figures related to the number of detected mobile phones in the studied area could also be duplicated (perhaps the same cell phone is detected more than once)

GDPR compliance

Data exchanged in this use case does not involve personal data, since in the early piloting stages citizens involved in the trials will not need to identify themselves to provide their input, therefore it presents no effects over GDPR.

The moment the pilot is stable and reaches a wider audience, it will probably need to implement a registration mechanism where the proper GDPR compliant measurements should be put into effect.

Requirements summary

Below we provide a summary of some functional requirements that have been elicited for the specific use case:

- The local architecture will be scalable and can be integrated with others.
- Deployed devices will not impact negatively in the scenario nor affect the daily operations as they are before their deployment.





- The associated web application should protect the privacy of the end-user and give the possibility of modifying the privacy parameters any time.
- The associated webpage should provide means to gather satisfaction information from the user.
- The application should provide a tool to analyze data and extract statistics in simple and easily understandable way for the city economic development division and for the event organizers.

Replicability, Complementarity and Impact

This Use Case could be easily replicated in any Smart City willing to have the kind of information it provides.

Use Case 1 is complementary to Use Case 6, being possible to integrate in the near future the information UC1 provides into the application UC6 will develop.



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

Description

The rapid increase of elderly population during the past years led by medical, social and economic advancements has become one of the most significant social transformation of the twenty-first century, and therefore, a worldwide concern and challenge for many countries.

According to data from World Population Prospects: the 2017 Revision, the number of older persons is expected to more than double by 2050 and to more than triple by 2100, rising from 962 million globally in 2017 to 2.1 billion in 2050 and 3.1 billion in 2100. Globally, population aged 60 or over is growing faster than all younger age groups (Nations, 2017).

Despite that older people are one of the fastest growing segment of population (due to the increase of life expectancy mainly because of medical progress and better life conditions), the lack of social relationships, either as a result of living alone or due to the lack of close family ties has conducted to the fact that many ageing people feel isolated. This should be considered as an important risk from the point of view that it could lead to a mental and physical decline. For example, lack of physical activity, poor cognitive performance and increased risk of dementia, depression, poor diet and so on.

On the other side, the biggest fear for many ageing citizens is to fall or become unwell without being detected or being helped for a long time.

As the current demographic shift which cities are suffering, where the number of elderly people is increasing year by year, and at the same time the exponential growth of IoT, expected by 2020 that will exceed 30 billion (the equivalent of 4 devices per person), this use case aims to provide a solution to improve quality of life of elderly population while at the same time ensure through the M-Sec platform a trust environment concerning all the sensible data and privacy protection collected by these devices.

Insulation affects more and more people, especially the elderly, impacting negatively on health and quality of life. As people age in modern big cities, the personal trusted networks that we develop throughout our lives weaken. This is a natural process that affects a large number of people around the world, but more especially in Europe and its population.

Loneliness is correlated with quality of life: older people who feel alone are more likely to refer to less satisfaction with life, compared to well-connected individuals; older people who are alone are more likely to experience certain problems:

- The probability of entering municipal residential establishments is 3.5 times higher than the average.
- The probability of visiting your doctor is 1.9 times higher than the average.
- The probability of having a medical emergency is 1.3 times higher than the average.
- The propensity to suffer depression is 3.4 times greater.
- The propensity to develop dementia in the next 15 years is 1.9 times greater.

Worldline will use its Connected Assistance platform as a starting point, a solution that already covers some issues related with health and wellbeing. Additionally, a range of functionalities will be added in order to



offer a complete solution not only on terms of wellbeing monitoring but also by making ageing people to feel safe at home through smart home sensors and less isolated through a video-call, chat tool so elderly people can stay longer and independently at their homes.

Additionally, it may be possible that a third pilot could be conducted on the city of Barcelona focused on measuring parameters related with health data (blood pressure, glucometer, and so on). This is mainly because the City of Santander government has no political competences over healthcare. However, at this stage of the project, we have not included on this deliverable as first we have to evaluate potential customers where the pilot could be carried out.



Home
monitoring



Loneliness and
social isolation



Physical & mental
wellbeing

Figure 13: Use Case 2 functionalities

Table 1: Use Case 2 description of potential measurements

Use Case 2 functionalities	Example of what to monitor/measure/perform
Home activity monitoring	<ul style="list-style-type: none">• Presence sensor• Window/door open sensor• Temperature sensor• Smart plug
Isolation and social isolation	<ul style="list-style-type: none">• Video-call, call• Chat• City activities
Wellbeing monitoring	<ul style="list-style-type: none">• Steps• Sleep• Bed occupancy sensor• Weight



Use Case 2 (Home monitoring & Wellbeing Tele-assistance for active and independent ageing people) will be composed of two different use cases involving two different user profiles and contexts. This is mainly to give an appropriate approach to each type of profile taking into account the survey performed. Therefore, there will be two different pilots to be conducted within Use Case 2. The following Table 2 summarizes their goal and coverage of the identified use case and who is the target user profile envisioned for each one.

Table 2: Use Cases scenario covered, implementation and target users

Use Cases	Use Case name	Scenarios covered	Where to Implement it	Target Users
Use Case 2.1	Tele-assistance	<ul style="list-style-type: none">Home Monitoring	City of Santander	Elderly citizen harnessing from social tele-assistance services + Family Network + Tele-assistance service
Use Case 2.2	Social & Physical Wellbeing	<ul style="list-style-type: none">WellbeingLoneliness and social isolation	City of Santander	Active elderly citizen living alone + Family Care giving Network

For Use Case 2, this consortium has decided to establish a multi-use case structure that distributes the focus on different stakeholder needs, namely:

- The City of Santander is currently providing a social service for elderly citizen, where the vast majority are older than 81 years old and live alone, that is run by a tele-assistance operator. The willingness from this stakeholder and the City of Santander Social Services responsible is for a digitalization of such service for the actual sensor measuring involved today (presence sensor, CO₂ sensor, emergency button and fall detection). Use case 2.1 will replicate somehow the current “analogue” service (provided via DTMF, Dual-Tone Multi-Frequency, protocol and radio-enabled devices).
Following the result of the survey from “tele-assistance users”, despite 50% have stated that they have a high technological level and are open to use new technologies, there is a big barrier on the use of IoT devices mainly because of the difficulty of use itself, as security and privacy concerns will be solved with the application of the M-Sec platform. In addition, 43% of the people surveyed have not done any internet search during the last month, denoting that this segment of elderly population is not familiarized with the use of technologies at all. Moreover, the functionalities with higher percentage of adoption correspond to emergency button, smoke detector, fall detector and electronic pills. However, emergency button and fall detector will not be included on this use case for security reasons as it may cause some confusion to the ageing people by having two replicated systems and not knowing to which one push. Therefore, there will be a specific use case (Use case 2.1) for this population segment, where only home monitoring alerts will be taken into account for the pilot, with the aim of replicating partially the current system that the tele-assistance operator have nowadays but in a digital way while providing the M-Sec security and protection layers.
- City of Santander, following the request and voice from their elderly citizens, has also decided to open a pilot track to monitor additional parameters related to well-being and social isolation that go beyond the



scope of current social services provided. Therefore, a differentiated client application and user panel will be focused in use case 2.2. The survey conducted to civic centre activities, users show that 62% of participants have a positive attitude towards the use of technologies and only 5% have stated that they have not done any internet search during the last month. Additionally, 45% of surveyed would use IoT devices and 52% would share the information collected with family network/caregivers. Activities on the city, wellbeing recommendations and a communication channel are functionalities that participants would like to have within the solution provided.

The following Table 3 summarizes the composition and context for each use case within the use case 2:

Table 3: Use Cases context and set-up

Use Cases	Who is monitoring or dynamizing	Set-up
Use case 2.1 Tele-assistance & Emergencies	Tele-assistance provider	<ul style="list-style-type: none">• Elderly homes will be set-up with different sensors and gateways connected to M-Sec platform.• Tele-assistance provider will be provided with a web front-end displaying enriched monitoring & emergency data from users.• Family caregivers will be provided with a mobile app to access the elder granted data.
Use case 2.2 Social & Physical Wellbeing	Santander	<ul style="list-style-type: none">• Elderly citizens will be provided with different wellbeing devices connected to M-Sec platform.• Elderly citizens will be provided with a mobile app for smartphones that will feature a communication channel (chat, video-call, call)) to address their beloved ones.

Interest

Today's world is undergoing an important technological transformation and IoT is one of the mainstreams that will drive important changes and cause a huge impact especially on the wellbeing industry.

While it is possible to find more and more a huge amount of applications in the marketplace related with health, care, wellbeing, meditation, social and so on, it is difficult to find a single one that cover all the aspects that elderly people may need in order to live by their own.





Table 4: Use Case 2 interest and motivations

Use Case 2	Interest & Motivations to use M-Sec
Use case 2.1 Tele-assistance & Emergencies	<ul style="list-style-type: none">• Improvement of data gathering and information enrichment with the digital transformation of the current local tele- provided by the city government, through the introduction of digital sensors and communications• Improvement of data security and integrity through M-Sec layers: components (sensors, IoT devices, cloud systems) involved in the data stream dissemination need to be tamper-proof to prevent from malicious attacks on devices• Data collected from IoT sensors must be authenticated as provided by the monitored subject to assure data proof-of-ownership at application level
Use case 2.2 Social & Physical Wellbeing	<ul style="list-style-type: none">• Tele-assistance services will be complemented with a new social service to fight social isolation and enforcement of wellbeing activities for a different set of Santander ageing citizens who are not harnessing from tele-assistance services but they need inclusive policies for their active and independent living.• Strengthen the personal relationships of the elderly so that they have more social interactions and, at the same time, create new groups of people over 65, making them participate in the community life of their environment.• The elderly citizen has two different networks: one for the people of their trust (family, friends, volunteers, neighbours, etc.), and that created from the City of Santander, which will be formed mainly by other elderly people and one group dynamizer. This facilitator is responsible for encouraging the elders that are part of the network to participate in the activities of their community and their environment.

Stakeholders involved and means of interaction/engagement

1. **Ageing People** (as data producer and data consumer)
2. **Relatives** (as data consumer to get information about a family member)
3. **Caregivers** (as data consumer to monitor patient's status)
4. **Social Services/Tele-assistance service providers** (as data consumer to monitor and track wellbeing and home user data).
5. **Dynamizer** (City of Santander) in some tasks within the pilots to promote and encourage participation of elders in the activities of the community

Some of these stakeholders have already been contacted. Some ageing people have already been contacted through questionnaires to get feedback about the solution to be provided on use case 2.

Further steps of interaction and engagement will be conducted on the pilot definition and through dissemination and communication activities (WP5).



Use Case Diagram

In this point, two different cases will be distinguished.

1. Use case 2.1 Tele-assistance & Emergencies

Pre-conditions:

- Tele-assistance service provider will monitor in parallel their current clients along with a small set of users that will be monitored by two means: the current analogue service and M-Sec sensors. These users will generate digital data secured by M-Sec platform and displayed in a different touch point (web client).
- M-Sec sensors set will be finally decided at pilot phase after evaluating the most adequate devices that fit with the current measures and will be installed in user's homes.
- The care giving network of elderly citizens (family) will be also provided with a mobile client application to monitor any potential event or emergency that may occur in their beloved homes.

Post-conditions:

- Deliverable 2.2 *"M-Sec pilots definition, setup and citizen involvement plan"* within this work package will define the KPIs designed to track the integration of the tele-assistance service with the M-Sec capabilities and functions in terms of security, usability, functionality and performance.

Functionality to deliver:

Table 5: Use case 2.1 Tele-assistance & emergencies features

Use case 2.1 Tele-assistance & Emergencies	Description	Target stakeholder & client front-end
Home activity Dashboard	<ul style="list-style-type: none">• General overview of KPI (<i>Key Performance Indicators</i>) and sensors that are under monitoring at elderly citizen homes.• History data view	<ul style="list-style-type: none">• Tele-assistance provider (web client)
Emergency Alerts	<ul style="list-style-type: none">• Alert triggering system warning stakeholders of unusual or dangerous events for the user	<ul style="list-style-type: none">• Tele-assistance provider (web client)• Family caregivers (mobile app)
Login/Registration	<ul style="list-style-type: none">• In order to access securely to user data, authentication must be implemented	<ul style="list-style-type: none">• Tele-assistance provider (web client)• Family caregivers (mobile app)





Basic Flow (UML diagram):

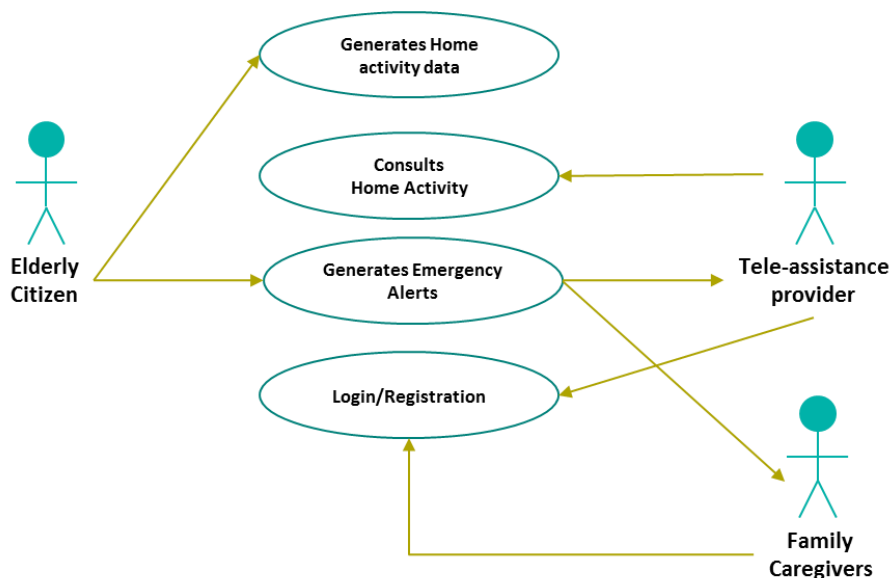


Figure 14: Use case 2.1 Tele-assistance & emergencies UML diagram

2. Use case 2.2 Scenario Social & Physical Wellbeing

Pre-conditions:

- In this pilot, elderly citizens and care giving network will be provided with a mobile app featuring communication capabilities to fight social exclusion and isolation (chat, video-chat and call). This client front-end will be managing wellbeing data related to physical and mental activity.
- No actual action will be derived from the collection and analysis of wellbeing data from users. City of Santander will be collecting the data but only for informational purposes.
- A new set of users will be selected from those elderly citizen living in Santander with a profile matching the following aspects:
 - Elderly citizen (above 65) living alone and owning a smartphone
 - Family relatives and/or other actors (friends, neighbours, community members) willing to participate as a care giving network and social contact for the elderly citizen
 - Acceptance and consent to participate in this pilot under the conditions expressed above
- Wellbeing (physical and mental) parameters will be defined in Deliverable 2.2 “*M-Sec pilots definition, setup and citizen involvement plan*” and thus the sensors or devices that will capture and communicate these parameters.

Post-conditions:

- Deliverable 2.2 “*M-Sec pilots definition, setup and citizen involvement plan*” within this work package will define the KPIs designed to track the integration of the tele-assistance service with the M-Sec capabilities and functions in terms of security, usability, functionality and performance.



Functionality to deliver:

Table 6: Use case 2.2 Social & Physical Wellbeing features

Use case 2.2 Social & Physical Wellbeing	Description	Target stakeholder & client front-end
Login/Profile registration	All users will have to register their profile in the mobile app to provide proof-of-access to data and features	Elderly citizens + Care giving network (mobile apps)
Wellbeing Monitoring	Physical activity (steps, weight, sleep quality) and mental exercising will be part of the parameters to monitor	Elderly citizens (wellbeing device) + Care giving network (mobile app)
Social isolation	Video-call, chat and call triggering from the app among care giving network and elderly citizen	Elderly citizens + Care giving network (mobile apps)
Wellbeing Dashboard	Display of monitored parameters	Elderly citizens + Care giving network (mobile apps)
Wellbeing activities	Activities and tasks to encourage the elders that are part of the network participate in the activities of their community and their environment (i.e. sharing their wellbeing data)	Elderly citizens (mobile apps) + Dynamizer/City of Santander (web client front-end)

Basic Flow (UML diagram):

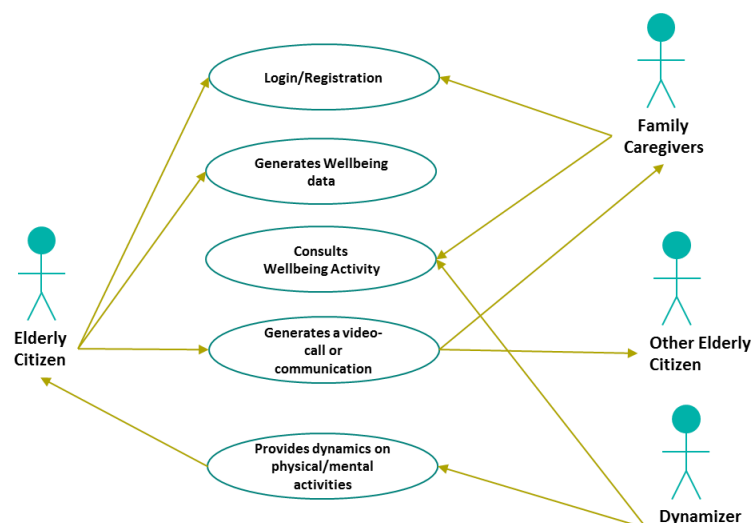


Figure 15: Use Case 2.2 Social and Physical Wellbeing UML diagram





Threats and Difficulty of realization

One of the challenges coming from this use case is the target audience. While the advanced on technology on the latest years has provided with new opportunities, the rate of technology adoption among oldest generations is still lower than other generations. This could generate a rejection to the use of the solution proposed or a difficulty on its appropriate use. As part of the actions to be taken into consideration on this use case, the pilot will be conducted not only to elderly users but also relatives and caregivers will be involved with the aim that citizens can feel supported on the use of the application and all the IoT devices used.

Another challenge is the one that comes about security's concern. With the increase of connected devices, new challenges in terms of information security appear. IoT deals with unprecedented volumes of private, real-time and detailed data. Personal data is a sensitive subject that users may not want to share if there is not guarantee about security breach.

On top of M-Sec project, the aim is to create a platform using the most advanced technologies (Cloud, Big Data, IoT Security, and Blockchain) to ensure the level of security and privacy in order to create a system that is trustworthy for stakeholders. Our aim is to create awareness about the benefits of the M-Sec platform not only when conducting the pilot, but also through dissemination and community activities.

Finally, the cost of the IoT devices along with the Hub, may be a threat in terms of adoption and scalability. For that reason, the idea is to involve relatives from the very beginner stage, so they can participate by providing them with the devices needed as a value exchange by benefiting from security and safeness of their family.

GDPR compliance

In order to get a different approach from the end user point of view, a questionnaire has been sent with aim to get a better understanding of requirements per part of the potential users. Survey has been conducted in anonymous form not including any personal data that may not comply with GDPR policy.

With respect to the use of Blockchain technologies within this use case, however, this topic will be covered in the definition of requirements for M-Sec platform and security layers designs in WP3 and WP4. This consortium is clearly determined to effectively integrate Blockchain security properties into this use case (i.e. multi-signature data access) and some strategies will be required to address the tension between GDPR and Blockchain. These tensions revolve basically around three issues that have not yet been conclusively settled down by the EDPB (*European Data Protection Board*) or in court:

- **Identification and obligations of data controllers and data processors:** there are many situations (in Blockchain platforms) in which it is complicated to identify a data controller to make them comply with their obligations. In such situations, that might lead to the use of private or permissioned Blockchain with regulated and identify actors for the transaction validation and processing.
- **The anonymization of personal data:** it essentially deals with what data is required to be stored in a Blockchain network. Is it actually required to store personal data, even if encrypted? Basically it is not. There is off-chain infrastructure that may serve as storage for personal data leaving the Blockchain capability and purpose for the data access transactional processing.





- **Exercise user rights regarding personal data:** GDPR states the rights to data erasure, rights to forgiveness, rights related to automated processing that are clearly difficult to exercise in a Blockchain environment given its immutable property. Again, strategies regarding which data shall be stored in a Blockchain will come up in the definition of the platform requirements.

Security requirements summary

Regarding personal data collected on the pilot, there will be a specific section within D2.2 “M-Sec Pilots definition, setup and citizen involvement plan” and within D5.11 “M-Sec GDPR compliance assessment report” [D511] explaining more in detail procedure for data personal treatment as well as Data Protection Officer pointed out. The following Table 7 depicts the main security requirements that will be specified for the M-Sec platform to provide in each of the pilots:

Table 7: Use Cases 2 security requirements

Use Case 2	Data security	Application Security	IoT/sensor security	GDPR compliance
Use case 2.1 Tele-assistance & Emergencies	<ul style="list-style-type: none">• Data encryption• Data access• Access control• Secure Communication	<ul style="list-style-type: none">• Biometrics and secure authentication	<ul style="list-style-type: none">• Tamper-proof device security• Device digital identity for authentication	Off-chain data storage
Use case 2.2 Social & Physical Wellbeing	<ul style="list-style-type: none">• Data encryption• Data access• Access control• Secure Communication	<ul style="list-style-type: none">• Biometrics and secure authentication	<ul style="list-style-type: none">• Tamper-proof device security• Device digital identity for authentication	Off-chain data storage

Replicability, Complementarity and Impact

The increase of ageing population is a global phenomenon. Not only in developed countries but also in less developed regions. This use case can be applied everywhere but specially it can be really useful for those living in rural and remote areas where users would be able to communicate with their relatives, caregivers or even doctors. The impact of M-Sec applications under this Use Case 2 will be relevant given the number of communities and regions with a reduced index of hospital bed per inhabitant or elderly communities living alone in their homes.

Scalable client front-end applications will be implemented to serve to the different pilots by filtering which data and sensors to showcase to supporting stakeholders. These applications will be developed as “white label” replicable assets that will be easily branded and customized to a different city and context through their front-end API.

Use case 2 can be complementary with use case 1 “Reliable IoT devices with multi-layered security for a smart city” in the sense that users can allocate IoT devices for environmental measures on their own residences in order to provide data that can be processed with the rest of home sensors at the Use case 2.1 Tele-assistance & Emergencies.





4.2 Fujisawa Use Cases

Fujisawa city (depicted in Figure 16) is about 50km from Tokyo, and it takes about one hour by train to get there. Its current population is 420,809 inhabitants and its total area covers 69.5 km². One of the most famous places in Fujisawa is an island, called Enoshima. Enoshima, in recorded history, had already flourished as a tourist spot in the Edo era. Fujisawa is the central city in “Shonan”, one of the most popular beach areas in Japan. It is known as a city of residence, sightseeing, business and education.

In addition, Enoshima is chosen in the sailing competition of the 2020 Tokyo Olympic and Paralympic Games as a venue. And in the same year, Fujisawa city will reach the municipal organization enforcement 80th anniversary. The city would like to utilize ICT to treat Olympic participants and visitors from all over the world, and lead this big event success in this memorial year.

The city and some of Japan’s leading companies established a smart town called “*Fujisawa Sustainable Smart Town*”. The plan is to apply comprehensive solutions for an entire house, entire building and entire town, combining energy technologies to provide a safe and secure environment. They will effectively create an advanced model of a town demonstrating efficient use of energy by promoting widespread use of energy-saving devices and proposing new solutions that integrate measures for energy creation, storage and management.

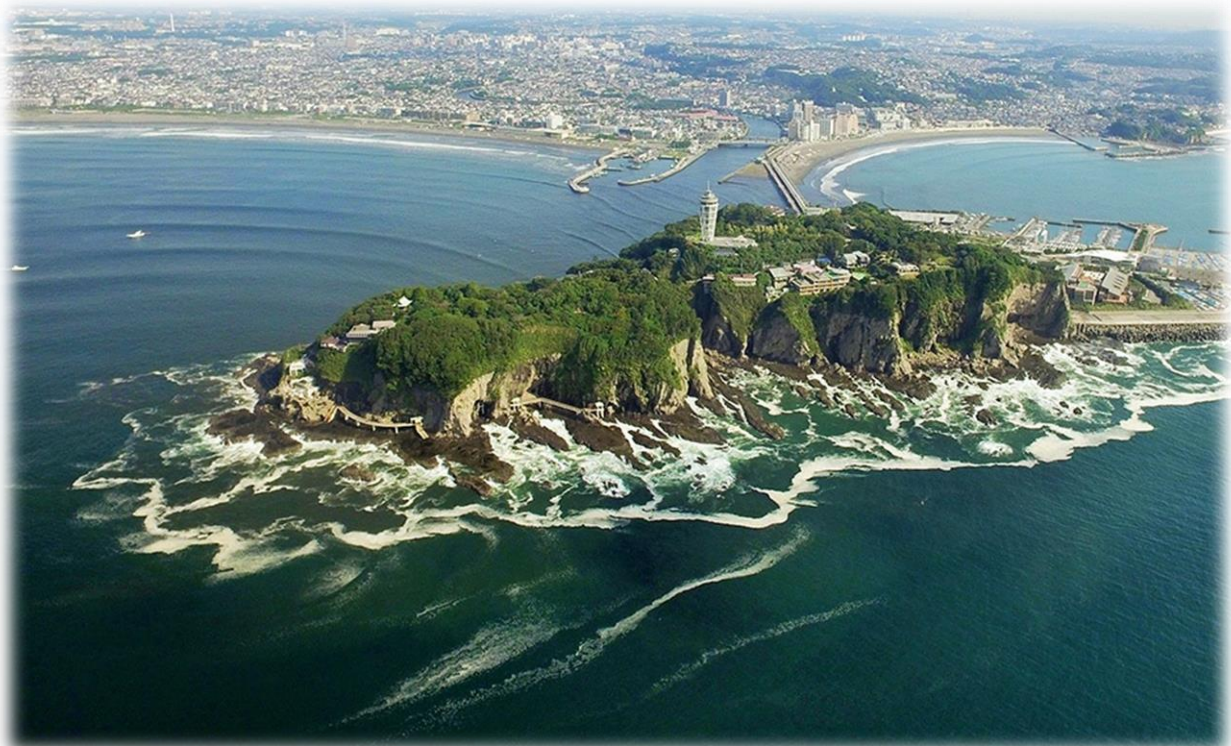


Figure 16: Aerial view of Fujisawa

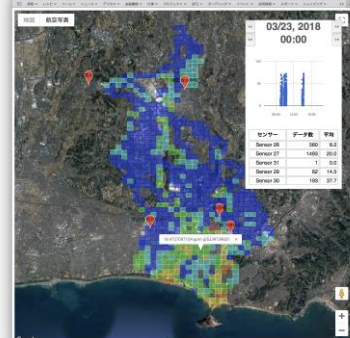
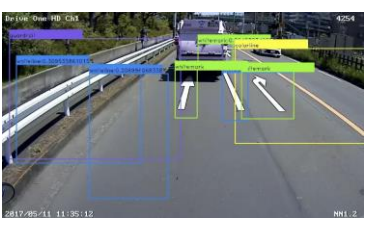



Use case 3: Secure and Trustworthy Urban Environment Monitoring with Automotive, Participatory, and Virtual Sensing Techniques

Description

Environmental data are one of the major pieces of information that enable people to optimize their behaviour. The data include, for example, air quality, road monitoring images, river monitoring images, and so forth.

Table 8: Examples of Environmental Data Captured in Use case 3

Data	Description	Sensors Used	Image
Air Quality	This data includes temperature, humidity, and the density of air pollutants, such as PM2.5. These data are collected spatially fine-grained way so that each citizen can optimize his/her travel in the city to avoid bad air quality. The following picture is a sample visualization of PM2.5 for each 100m x 100m grid area.	This data, and the following data also, is collected mainly by the automotive sensing platform . Public vehicles are operated all through the city with embedded air quality sensors. The sensors emit at least one set of sensor readings during their operation.	
Road Monitoring Images	This data is captured to detect damages on/along roads. The damages on roads typically contain damaged paintings, potholes, etc. Those along roads are in most cases damaged guard rails.	The data is generated from images captured by the camera attached to public vehicles. Images are processed using machine learning techniques either at the vehicle's side or at the cloud system's side.	
River Monitoring Images	This data is captured to enable local governments to react to almost-flooding river when it is hit by a huge storm, e.g., a typhoon.	The data is collected using virtual sensing mechanism, which periodically scrapes the pieces of information of interest from web pages. It may also be captured using a participatory sensing mechanism.	





This use case entails a client application that allows urban environment monitoring entities, for example local governments, to visualize dense environmental data spatially and temporarily. Using the application, the entities are enabled to better serve their citizens with sophisticated environment monitoring data.

The automotive sensing platform generates real-time sensor data streams and participatory "*human sensors*" data from all over the city leveraging a hundred mobile sensing trucks and thousands of human sensors. The mobile sensing trucks in Fujisawa City mainly consists of tens of garbage collection trucks, shown in Figure 17, operated all through the city in weekdays. "*Human sensors*" are city officers who make reports on their findings in the city. The reports are about graffiti, smelliness, noisiness, etc., which all can only be detected by human sense. Those officers are considered to be the participants to these sensing projects, therefore this form of sensing is termed to be *participatory sensing*.



Figure 17: Automotive Sensing Trucks in Fujisawa City

The environment data, including those mentioned above, become particularly important when a disaster hits a city; for example, when a typhoon hits a city, its government needs to precisely monitor the water level of river using sensors and cameras. If sensors, IoT devices, and cloud systems involved in those data streams are attacked, the users are unable to acquire the authentic information, which causes their lives to face danger. However, the aforementioned mobile sensing platform is now in operation without any security/privacy concern. Therefore, the following objectives need to be achieved.

1. The heterogeneous components involved in the data stream dissemination need to be secured so that they are not compromised by malicious attackers.
2. The data streams need to be secured so that the data are not tempered in the network between their source and destination.
3. The data streams should not harm citizen's privacy, thus an automated privacy protection mechanism should be provided.
4. The data, when they are accumulated to form a dataset, should be circulated via a marketplace so that they are analyzed together with other data.



Interest

Environment monitoring is one of the major tasks of local government. Better serving citizens with live environment data contributes to wellbeing of the society. This use case illustrates how environment monitoring data can be captured from the real world, handled in the cloud system, and delivered to citizens securely.

Environment sensing data, namely sensor data and camera images, are encrypted so that they are not tampered. IoT devices and cloud systems are monitored to protect them from malicious attackers. The data is, in case they are provided to applications in an open fashion, disseminated through the data marketplace leveraging the Blockchain mechanism. In all, data authenticity, data security, IoT device security, and cloud systems security are achieved to ensure secure and trustworthy environment sensing and data dissemination. The data is provided to (1) city government in encrypted form and (2) a number of applications via the marketplace.

Stakeholders involved and means of interaction/engagement

The major stakeholders in this use case are (1) data supplier and (2) data consumer. The following concrete stakeholders have been identified for the specific use case:

- **Fujisawa City** (data consumer and supplier)
Local government leverage the data to better serve citizens. It also supplies the data as it operates garbage collection trucks, the automotive sensing platform.
- **Fujisawa Recycle Coop** (data supplier)
Fujisawa Recycle Coop also operates garbage collection trucks, the automotive sensing platform. Its employers act as participatory human sensors.
- **Citizens** (data consumer)
Citizens are major data consumers who try to optimize their behaviour based on the data.

The majority of these actors have already been contacted concerning the M-Sec project. At least one physical meeting per stakeholder will be organized with the participation of the Fujisawa City and KEIO. A clear interest in the results of the project has been identified. They include, but are not limited to, real-time monitoring of the city with data trustworthiness, compliance to privacy protection regulations, and insightful visualizations of the city.



Use Case Diagram

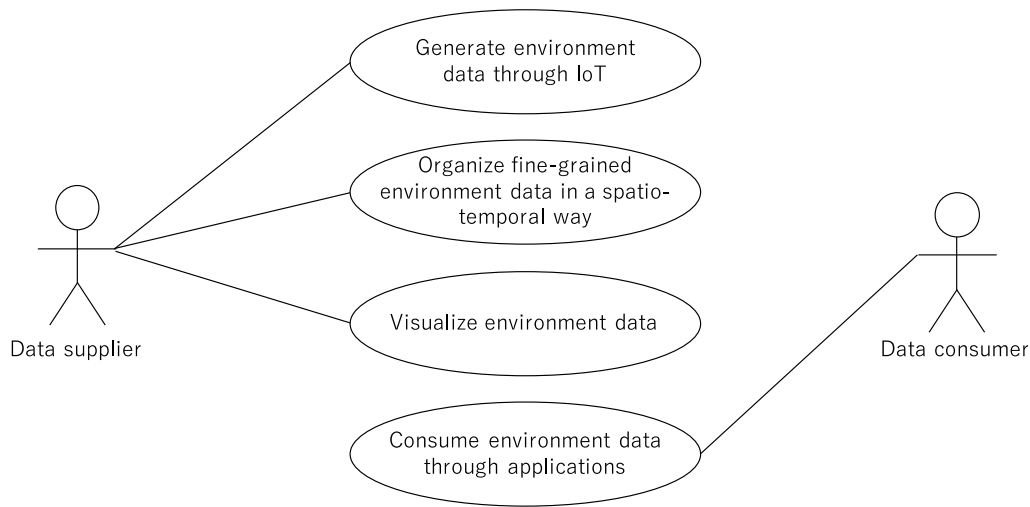


Figure 18: Use Case 3 UML Diagram

Threats and Difficulty of realization

If sensors, IoT devices, and/or cloud systems involved in this use case is/are compromised, they will generate unauthentic and in most cases incorrect data. For example, if an IoT device, which detects flooding river from a camera is compromised, it may always generate the data that mean the river is not flooded. On the other side, data consumers have no means to know whether those devices are compromised or not. Therefore, they may risk their own life being unaware of the flooded river due to the misinformation.

To cope with this threat, one of the challenge in this use case is to clarify whether or not the devices are compromised. Such information enables consumers to know whether the data they see are safe in terms of data authenticity. Another challenge is to protect the data itself. If the data are, for example, encrypted at the edge side, they are protected from malicious attackers even if the cloud system is compromised. It is also a challenge that we better protect privacy information. If a camera image contains private cars with their numbers and/or individuals with their clear faces, their privacy may be leaked. In these three layers, namely device, data, and data content, secure and trustworthy environment monitoring should be made.

GDPR/PIPA compliance

Data exchanged in this use case does not involve personal data, therefore it presents no effects over GDPR. Interaction with citizens will be made anonymously.

Requirements summary

Below we provide a summary of some functional requirements that have been elicited for the specific use case:

- The local architecture should be scalable and can be integrated with others.
- The system in all should not harm user privacy.
- Deployed devices will not impact negatively in the scenario nor affect the daily operations as they are before their deployment.



- The associated web application should provide and visualize environment information collected over the city.
- The application should provide a tool to analyze data and extract statistics in simple and easily understandable way for the city environment division and citizens.

Crosscutting these functional requirements, Table 9 summarises security requirements of this use case.

Table 9: Use Cases 3 security requirements

Use Case 3	Data security	Application Security	IoT/sensor security	GDPR compliance
Secure and Trustworthy Environment Monitoring	<ul style="list-style-type: none">• Representing data authenticity• Data encryption• Data Access control• Secure Communication	none	<ul style="list-style-type: none">• Light-weight Intrusion detection in IoT devices• Tamper-proof device security	none

Replicability, Complementarity and Impact

This use case is replicable in other cities, especially cities where citizens suffer from air pollution. In one aspect, sensors and IoT devices used in this case should easily be leveraged in a number of cities. In the other aspect, which is more important, the application, the systems running in cloud and edge sides, and the security/trustworthy mechanisms for them can be ported adaptively to systems of other cities. To this extent, we will make the following resources open on the project website, so that the use case is replicable in other cities. First, the cloud-side system that exchange sensor data stream between data suppliers and consumers will be made open. Third party developers can download the software, and deploy it for their own cities. Second, applications built for this use case will be made open, too. These can be used as a reference and also as they are. Finally, the software running in the edge-side, namely IoT devices, will be made open. All together, we will establish a replication basis in our project. The replication requires cooperation by citizens or the local government to operate environment sensors. When the scenario is used in a heavily-polluted city, it has a huge positive impact to the citizen's wellbeing, which is dealt with in use case 2.





Use case 4: Secure and Trustworthy Hyper-connected Citizen Care

Description

In this use case, “*Hyper-connected citizen care applications*” will be created for a range of different purposes and for different stakeholders. On one hand, government officer’s application collects data on the city, such as urban waste generation per household, pedestrian flow or traffic flow data, through the M-Sec architecture and analyze the data to elaborate value-added data that affect citizens efficiently. Citizen’s applications, on the other end, consume that value-added data to empower their decision on related topics towards better (physical, mental or social) wellbeing or QoL (Quality of Life) in their daily lives.

Here, suppose exchange of information under the Personal Information Protection Act (PIPA) and GDPR. For example, in case of certain international events in the city or high sightseeing seasons, we want to grasp the numbers and rough profile of visitors towards better support (e.g., people with disabilities) In order to do that, we need to securely acquire necessary and highly-secure data show those data in real time towards further analysis and applied services.

Therefore, the following objectives need to be achieved.

1. Any information related to personal identity must be secured so that it does not harm privacy.
2. The heterogeneous system components involved in the data stream dissemination need to be secured so that they are not compromised by malicious attackers.
3. The data streams need to be secured so that the data is not tempered in the network between source and destination.

This use case allows various urban environment monitoring entities (such as the local governments) to collect spatially- and temporarily-dense urban data (such as traffic or urban waste data) by using a number of mechanical/human sensors. Using the collected data, the entities are able to better serve their citizens with sophisticated monitoring data.

Interest

For hyper-connected society citizens, sophisticated applications are key to make their lives smarter.

For local governments in such a society, the applications are the means to affect citizens. In those applications, particularly in case they are provided by local/national governments, the information provided by the applications must be authentic and trustworthy.

For example, let's suppose an application that predicts citizens flow for better city management. This application acquires data that show the national character of foreign countries, make multi-ethnic people flow prediction, and use it for relieving pedestrian congestion at events etc. and planning for arrangement of facilities. Another example application is urban waste management, in which the amount of daily waste generation is sensed household by household, the resulting data are used for building serious game towards reduction of the amount, and citizens are enabled to understand their lives in terms of waste generation.



In doing these, the data (1) must be available for the government to provide stable and effective service, confident to protect personal information, and (2) must be integral for ensuring governmental decision based on authentic data.

Stakeholders involved and means of interaction/engagement

The following stakeholders have been identified for the specific use case:

- **Fujisawa City** (data consumer and supplier)
Local government leverage the data to better serve citizens. It also supplies the data as it operates garbage collection trucks, the automotive sensing platform.
- **Fujisawa Recycle Coop** (data supplier)
Fujisawa Recycle Coop also operates garbage collection trucks, the automotive sensing platform. Its employers act as participatory human sensors.
- **Citizens** (data consumer)
Citizens are major data consumers who try to optimize their behaviour based on the data.

The majority of these actors have already been contacted concerning the M-Sec project. At least one physical meeting per stakeholder will be organized with the participation of the Fujisawa City and KEIO. A clear interest in the results of the project has been identified.

Use Case Diagram

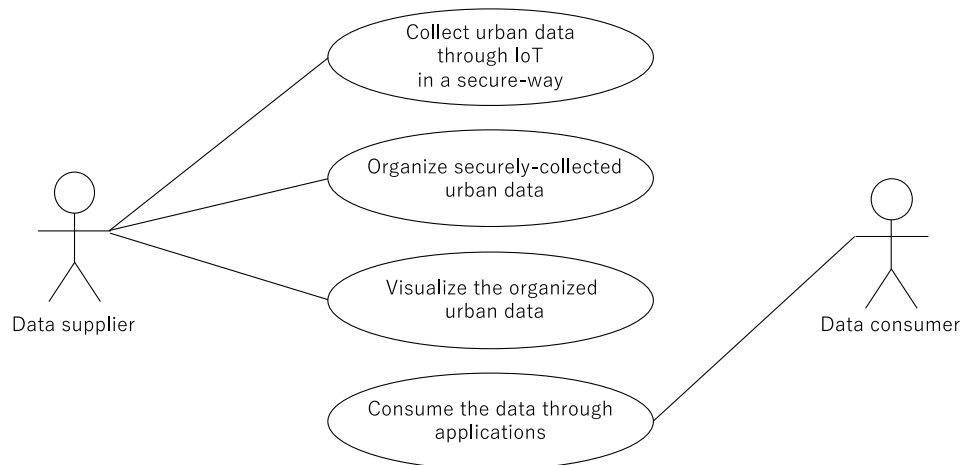


Figure 19: Use Case 4 UML diagram

Threats and Difficulty of realization

Firstly, if sensors, IoT devices, and cloud systems involved in those data streams are attacked, the users are unable to acquire the authentic information, which causes their lives to face danger. If a piece of data containing personal information is publicly distributed, his/her privacy leaks.

Secondly, if sensors, IoT devices, and/or cloud systems involved in this use case is/are compromised, they will generate unauthentic and in most cases incorrect data. For example, if an IoT device, which counts the



number of people from a camera's image is compromised, it may always generate the data that mean the number of people in the specific area is "zero" (or significantly lower number of people than the reality) even in case of a big event with huge number of audiences is going on. On the other side, data consumers have no means to know whether those devices are compromised or not. Therefore, they may risk their own life, being unaware of the large number of the audience located in the area and go to that area, and this eventually leads to an excessively-crowded dangerous situation. As an example of this, don't forget the Mirai botnet that in October 2016 used compromised IoT devices to launch DDoS attack [MIR].

To cope with these threats, one of the challenges in this use case is (1) to clarify whether or not the devices are compromised. Such information enables consumers to know whether the data they see are safe in terms of data authenticity. Another challenge is (2) to protect the data itself. If the data is, for example, encrypted at the edge side, it is protected from malicious attackers even if the cloud system is compromised. (3) Protecting privacy information is yet another challenge. If a camera image contains private cars with their numbers and/or individuals with their clear faces, their privacy may be leaked. In these three layers, namely (1) device, (2) data, and (3) data content, secure and trustworthy environment monitoring should be made.

GDPR/PIPA compliance

Data exchanged in this use case may contain possible personal data. One example is the amount of waste generation at each house-hold by capturing the number of garbage plastic bags collected from each house in a city. (This information is originally observed by local government officers, and this use case enables them to acquire it as digital data) Since this use case will be conducted in Japan, this use case will be complying with "Personal Information Protection Act" (PIPA). The PIPA compliance seems to be equally achievable through anonymization and encryption methods; nevertheless, the specific way to proceed is under discussion and will be polished in the following stages of the project development.

Requirements summary

Below we provide a summary of some functional requirements that have been elicited for the specific use case:

- The local architecture should be process securely.
- Obtained data need to be securely and appropriately protected.
- Data itself should be appropriately protecting the user's privacy.

Replicability, Complementarity and Impact

This use case is replicable in other cities that want to empower citizen's decision making based on securely sensed data. For example, in case of waste amount monitoring example, especially cities where the local government needs to reduce the amount of urban waste would be targets of replication. The urban-waste data would change the citizen's behaviour. The local government and society, in turn, would be enabled to reduce air pollution due to incineration using the waste data.





4.3 Cross-border Use Cases

One of the most challenging aspects of the M-Sec project is to implement use cases that will promote the cross-border synergies of the participating partners. This will bring closer citizens and smart city stakeholders from both sides. To this end the consortium has already identified some preliminary use cases that were introduced in the proposal and are expanded in this section.

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

Description

This use case is to construct a marketplace to distribute data by ensuring Confidentiality, Integrity, Availability, and Privacy of data following GDPR/PIPA regulations, so that people or organizations in EU and Japan can utilize the data more effectively. Recently, we see so many data collected from various methods such as human data, environmental data, industrial data and so on. However, most of them are buried or unused in the society even though it could be valuable and sellable to any organizations or people. One of the big reasons why they are not used or sold is that we do not know what and how we can exchange in a proper way. Although there is a way to do so, it is still not popular and most people even don't know that it exists, or it is not trustable enough in terms of security.

Furthermore, when we talk about international data distribution, not only technical issues but also legal issues arise, that is why the practical use of data market place among the general public has not been done. In this scenario, we will try to build a rudimentary mechanism of a data marketplace for citizens, businesses and others can trade data safely. At first, we set up one marketplace and accumulate data collected from citizens, companies, organizations, data automatically collected on the web, data collected from IoT terminals, with applying Blockchain technology and security measures at multi-layer. We aim that the results of this research and development will be utilized in various industries by constructing a mechanism that is the basis of data market place. The target of data sale is assumed to be citizens, companies, local governments, but first we will try to gather data.

- Local government data: data such as photos collected by staff by day-to-day operations, data of citizens whose secondary use of data is accepted.
- Data from citizens and visitors: Health data collected by pedometers, personal data collected by smartphones, data and collected by questionnaires.
- Data on the Web: Data automatically collected (environmental data, etc.)
- IoT data: data collected from IoT devices (cameras, etc.) owned by companies and local governments.

Interest

Why cross border data trade? Foreign visitors are increasing around the world. Business opportunities are expected in various industries and in municipalities the requirement of corresponding to foreign visitors are increasing. In such circumstances, the way of the data distribution between countries needs to be safely and smoothly done to make the data effective to contribute to make the smart city. For example, collecting the behavioural characteristics by nationality will be possible to use the data for an accurate marketing activities



and countermeasures against inbound visitors from that country. Specifically, the average walking speed of a citizen, the route selection, and the tendency of using stores will be collected from device/application, so the companies which need the data of the specific nationality will purchase data, or the municipalities might need the data for security planning and congestion mitigation measures in large-scale events tailored to behaviour patterns. Furthermore, when companies plan to advance into overseas markets, they will purchase market data of their specific target area to make a strategy. Along with the development of the Internet in recent years, since cyber-attacks are becoming increasingly complicated and sophisticated, provision of a secure data distribution method between international countries is an essential task for smart cities. For example, a terrorist may attack the data marketplace and tamper with activities data of people in an event by changing the arrangement of guards for the sake of terrorism. We aim to construct a marketplace where data integrity is present or tamperproof data can be securely distributed.

Stakeholders involved and means of interaction/engagement

- Data supplier
 - Citizens and visitors
Citizens and visitors provide data such as activity data or purchase data into the marketplace.
 - Municipality
Municipality provides data of citizens whose secondary use of data is accepted. The data can be used to attract companies to their city.
- Data consumer
 - Event organizer
Event organizer will use people activity data to make a guard plan or venue arrangement. They manage the event and promote visitors to provide data.
 - Companies, Chamber of commerce
Companies will use data in the marketplace to understand the behaviour of their target users and make a strategy for sales or overseas promotion.



Use Case Diagram

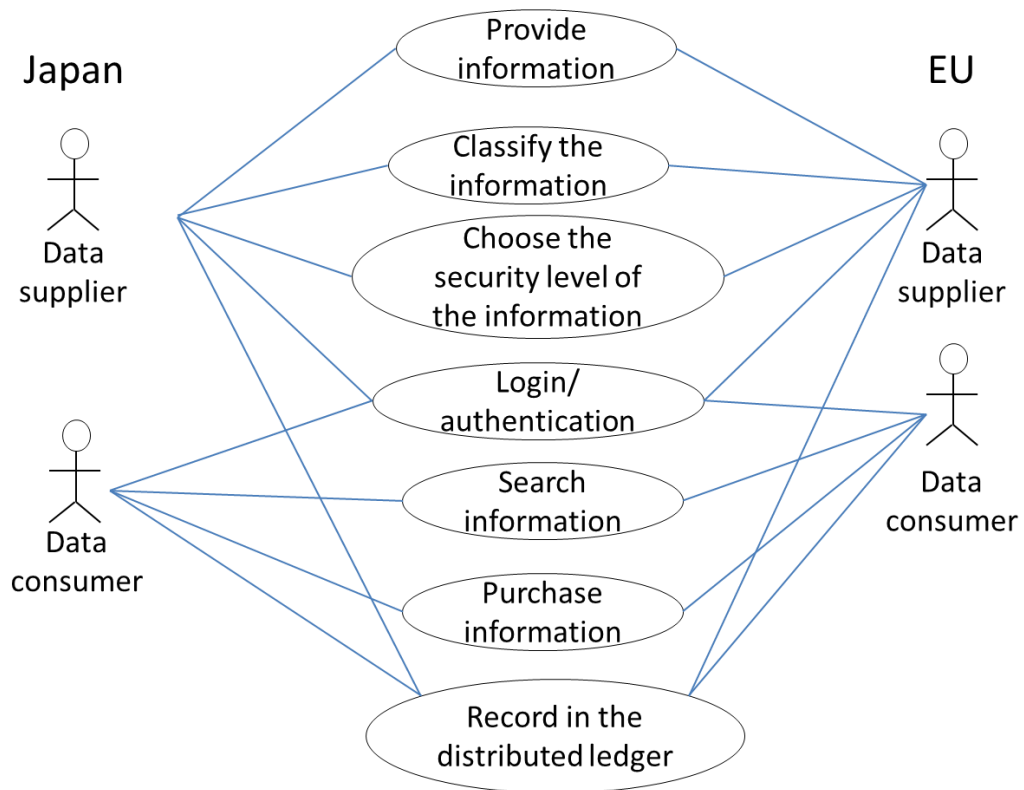


Figure 20: Use Case 5 UML Diagram

Threats and Difficulty of realization

Even though we will try to study methods in a form that conforms to GDPR and Personal Information Protection Act law as it says in the next section, there are possibilities not to be approved by governments since the method of anonymization and encryption are clearly shown for now. And not many users participate in events nor agree to provide their information as users will be concerned that their data, especially their personal data, might be used illegally. There is also a possibility that not many companies participate in the marketplace even though data are collected. It is necessary to consider and clearly explain the advantages of using cross-border data and promote candidate user companies to take part in the marketplace. Technically, safe and secure information security by using Blockchain techniques are concerned, but it is necessary to consider the secureness of multi-layer security, which will be discussed in WP3 and WP4.

GDPR/PIPA compliance

We will study whether the data created by anonymization and encryption methods could be utilized and distributed in compliance with GDPR and Personal Information Protection Act law, however, this topic will be covered in more detail within deliverable D2.2 and WP5.





Requirements summary

- The local architecture should be process securely.
- The cloud system should store the data securely and could be accessed from EU and Japan.
- The devices should be used to collect user's data such as behaviour characteristic data.
- The Blockchain technology to secure the data

The above will be the considered requirements within the consortium members and also stakeholders and end users. The assets researched in WP3 and WP4, as the Blockchain technology by ICCS, and SOXfire, web sensorizer and GANonymizer by Keio, for the marketplace are assumed to be used.

The following Table 10 summarises the security requirements of this use case.

Table 10: Use Cases 5 security requirements

Use Case 5	Data security	Application Security	IoT/sensor security	GDPR compliance
A marketplace of IoT services for effective decision making	<ul style="list-style-type: none">• Data Integrity• Data Access control• Secure Communication	<ul style="list-style-type: none">• Secure authentication	<ul style="list-style-type: none">• IoT device security	<ul style="list-style-type: none">• Off-chain data storage

Replicability, Complementarity and Impact

There are many cities that want to attract companies to their region. Moreover, there are many companies thinking about overseas expansion. Therefore, this use case can attract various industries and also anywhere. For companies planning to expand overseas, it will be an appealing data which can be achieved without going to the city. Conversely, for cities that are thinking about attracting companies to the region, the opportunities to attract companies will increase by providing their data. However, it will only be replicable as long as the laws and institutions of data handling in a particular country are organized, and WP3 and WP4 asset availabilities can be used as it is or if not, only if there is a method that can be added and repaired to be used. The discussions have been started between WP2 members including city partners. It will be planned to install in Fujisawa first and Santander after that to examine if it is applicable both in Japan and EU.





Use Case 6: Citizens as sensor

Description

This use case takes into account the current knowledge and habits of citizens in both Santander and Fujisawa in order to promote a participatory environment in which they contribute to reflect the pulse of every city, reporting on various events (state of the public road, traffic incidents, etc.), as well as quantitative measures of physical sensing provided by sensors that incorporate current Smartphones.

In this sense, the citizen who wishes can voluntarily contribute with the sending of information, making use of any of the categories (beaches, parks and gardens, transport, public roads, culture, sports, etc.), inserting images, including comments, date of the event, expiration date, etc. When users report the occurrence of such events, they will subsequently be propagated to other users who have subscribed to the respective type of events. The events under the responsibility of the Municipal Services are sent to the Town Hall as incidences for their resolution, thus enabling the citizens to know the state of the same ones at any moment.

In addition, there is a chance the different sensors commonly integrated in any mobile device could be used by the envisioned application to provide additional physical sensing information, always with the consent of the users. Citizens involved in the ulterior trial would have the chance of receiving rewards based on their participation, creating a game involving users from both cities. Furthermore, visitors of both cities can generate content for Fujisawa and Santander and benefit from taking part in the initiative. These rewards could be enjoyed in any of the cities participating in the rehearsal.

The information is shared with the rest of users through an App for mobile devices and is also available on the website of M-Sec, so that any citizen can know the pulse of the cities at any time, through this alternative information channel.

The sending of information can be done anonymously, thus not requiring a user registration process in which it must include personal data, or through the employment of a virtual ID created specifically for this service. In the latter case, a rewarding mechanism will be created to grant prizes to the most participatory citizens and considering it a proper mean to incentivize participation. Both the physical sensing information and the events sent by users are stored in the data repository of the M-Sec project, being used for the development of this initiative.

Interest

This application allows citizens to establish a new channel of communication with the administration and with the rest of neighbours, by sending photographs, notices and alerts on topics of interest. Therefore, they feel more deeply their involvement in the daily evolution of their cities and this helps to create a stronger bond among them and the city and develop a sense of community. Furthermore, this tool enables users to subscribe to a certain type of events and interact with each other based on those subscriptions.

In addition, from the Municipality point of view, it is a good way to create actions and promote initiatives attending citizens real demands and not only based on the municipal services and their technical partners beliefs, which sometimes could not reflect and address real problems faced by the citizens.



This use case presents a scenario where citizens from both involved cities can not only check what is happening in the other side of the globe but also sets up a playing field where those citizens can compete and obtain rewards based on their participation.

Stakeholders involved and means of interaction/engagement

- **Citizens:** participation and collaboration with municipal services through ICT, being end users of the solution.
- **Municipal services:** Offering online and real-time information to citizens on the status of municipal incidents from start to resolution. Therefore, the solution aims to achieve more efficient services.
- **Fujisawa and Santander Smart Cities:** providing their IoT infrastructure to conduct the trial and feed data in those cases where the information provided by sensors may supplement the citizen's perception.
- **SMEs and Research entities in the consortium:** Exerting as service providers and integrators, developing new application services to be employed by citizens and municipal services taking as a reference the interests presented by the municipal authorities, which in turn are influenced by citizens, taking advantage of surveys such as those carried out at this stage of the project.

Use Case Diagram

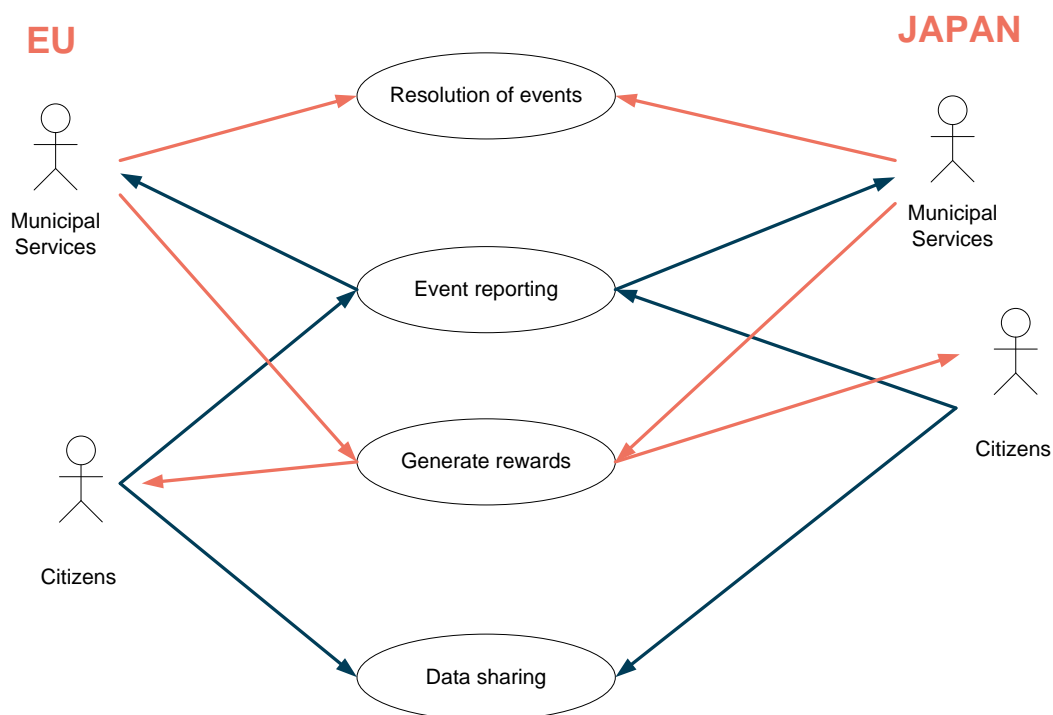


Figure 21: Use Case 6 UML diagram





Threats and Difficulty of realization

The main threat to the proper development of this use case is in its acceptance by citizens. If they are not willing to participate it will be really difficult to get valuable feedback.

- Low number of app downloads.
- Low amount of events reported.

In addition, participants could feel the rewarding systems is not working properly and express their dissatisfaction to the Municipalities, generating an overall bad impact over the initiative. Thus, the proper definition of what will be rewarded and how this reward will be distributed to participants must be accurately defined at the time when users register as participants in the pilot experience.

On the other hand, the municipal services will potentially get a rough scrutiny related to the way they act upon the reception of certain event:

- Reaction time to solve events.

Last but not least, the misuse of the application functionalities must not be overlooked:

- Users share rude pictures or comments.
- Users share pictures from an event where people can be identified

GDPR/PIPA compliance

In the EU side, the GDPR compliance is not difficult to achieve since one set of users will provide an online consent in order to start using the application, which in addition will not need of a registration process, thus not requiring to handle sensitive personal data. On the other hand, those users opting out for registering and creating a virtual ID, which in turn will be linked to the rewarding mechanism, will be subjected to a more refined scrutiny, getting GDPR compliance through anonymization and encryption mechanisms and having them signing and informed consent beforehand.

In the JP side, the PIPA compliance seems to be equally achievable through anonymization and encryption methods; nevertheless, the specific way to proceed is under discussion and will be polished in the following stages of the project development.

Requirements summary

This use case elicits some particular requirements such as the following:

- The cloud system should store the data securely so that they are not disclosed to any party without permission.
- The associated application should provide and visualize environment information collected over the city.
- The application should provide a tool to analyze data and extract statistics in simple and easily understandable way for the municipal services and citizens.



Replicability, Complementarity and Impact

This use case is easily replicable in any smart city willing to get a direct involvement of its citizens in their daily operations. Starting with this trial in Fujisawa and Santander, the developed solution will be put to a test in a real-life context and properly polished by citizens used to collaborate in these kinds of initiatives. Therefore, the time the project comes to an end the pilot experience will allow the consortium to offer a complete solution to other cities which might be interested in importing it, easily adapt it to every particular environment and incorporating their citizens to the rewarding program and thus achieving a experience that affects people in several parts of the globe.

The current trend to put the focus of the smart city evolution in its citizens is fully apprehended by this use case, so its impact in society is clear.

With regard to the complementarity, this use case might find common ground with M-Sec Use Case 1, where certain relevant events related to sensor measurements could be reported by citizens, thus helping municipal services not to rely exclusively in cold data but also in the citizen's opinions and comments. In relation to them, their participation in this use case execution will determine to a great extent, decisively in fact, the impact of the initiative. In order to achieve this high participation, the consortium will need to not only develop attractive functionalities in the app, but also to prepare and conduct strategies that attract citizens, such as conducting local promotional campaigns, holding dedicated workshops and establishing an attractive rewarding program.



5. Conclusions

The goal of this deliverable is to document the diverse use cases that are considered to create real-life pilots in M-Sec pilot sites, namely the Smart Cities of Santander and Fujisawa, which validate the concepts and developments of the project.

The analysis starts with a definition of the M-Sec concept itself, including an overview of the use cases as envisioned in the DoW and the main stakeholders involved, better understanding the context of the project and identifying the various stakeholders who represent a holistic value chain. This identification process is an important part of the scenarios definition process and during its course the following groups are considered as the primary M-Sec stakeholders:

- Administrations.
- Citizens.
- Small and medium enterprises with a technological background.

An introduction to how the consortium described use cases follows, detailing the templates employed and giving a hint on how the views from the diverse stakeholders considered were retrieved, letting readers get a grasp of the internal process followed by the consortium members when deciding what kind of topics were interesting to address.

This section leads to a more complete introduction of every use case, complying with a unified approach that starts with a brief description of that scenario, followed by a collection of thoughts on what is the interest behind its execution. Then, a list of stakeholders who may be interested in every particular use case, along with their implication appears, as well as a reflection on the kind of difficulties that may appear along the way. Finally, a succinct compilation of requirements and a short reference to the way in which it is intended to respect legality in terms of privacy and data protection wrap up the analysis

In addition, the reusability of components between the pilot sites is an important aspect addressed in this document. The main outcome of this exercise is the list of common services and developments that can be used at different pilot sites. Using this approach, the cities will be able to leverage implementations done at other sites thus increasing efficiency of the deployments. A profile of these users will be analyzed in further detail in future reports.

All in all, a complex scenario has been discovered and probably the discussion will have a growing approach while better understanding the citizens and public administration attitude toward the use of tools and technologies such as the ones presented by M-Sec. One of the key success factors is definitely the confidence in a clear privacy and data security assessment.

The definition of pilots to conduct these use cases will be the next step to take and it will completely shape the procedure M-Sec follows to bring its ideas and goals to real life. This analysis will be considered the focal point of Deliverable 2.2, which immediately follows this one.



Annex 1 – Use Case Surveys

Use Case 1 Survey

M-Sec Use Case 1

Horizon 2020 is the largest research and innovation programme in the European Union with a budget of almost €80 billion for the period 2014-2020. Its main objective is to ensure Europe's global competitiveness by funding research and development activities. It is open to the participation of research centres, universities or companies from any country in the world.

Within this innovation programme is the "M-Sec" project formed by a consortium of twelve partners (six European and six Japanese), which began last July and will run for 36 months. The main objective is to create a platform using the most advanced current technologies, to guarantee and ensure the integrity and confidentiality of all data/information collected through the Internet of Things (all those devices connected to each other capable of collecting and exchanging data, for example, appliances, lights, thermostats, air quality sensors, humidity, smoke detection, watches or intelligent wristbands, etc.).

One of the pilots being worked on and to be developed in the city of Santander involves the deployment of a series of novel IoT devices in selected locations in the city to both retrieve interesting environmental data along with a measurement of noise level while on the other hand will also be capable of sketching heat maps, using as a source of information the number of mobile phones in the area.

* Required

Email address *

Your email

Thanks for your participation!



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

Figure 22: Use Case 1 Survey Introduction





Participant profile - Age *

☐ 15-30

☐ 31-45

☐ 46-60

☐ 61-75

☐ +76

Participant occupation

☐ Municipal official

☐ Local resident

☐ Staffer of a private company

☐ Researcher at the University or a research center

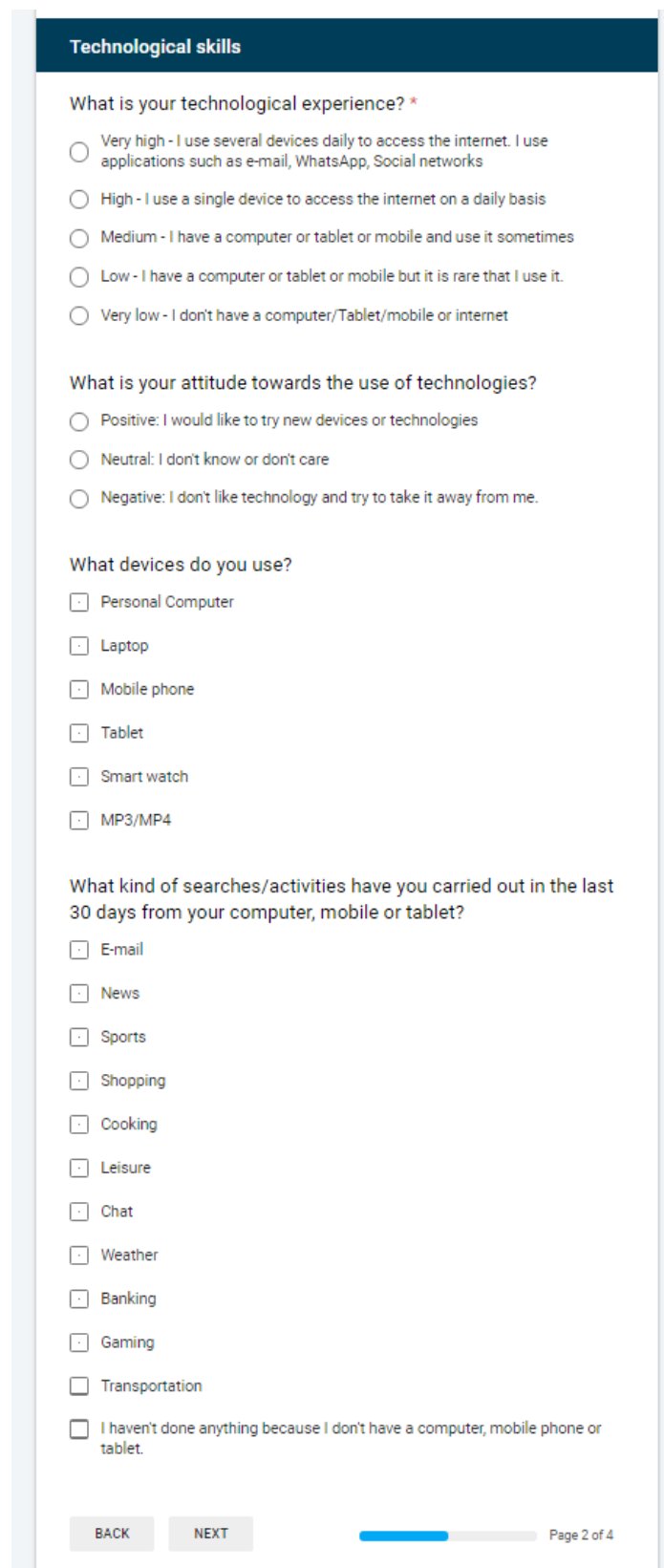
☐ Other: _____

Page 1 of 4

Never submit passwords through Google Forms.

Figure 23: Use Case 1 Survey Step 1





60



Security & Privacy

Tell us what you feel is a threat by introducing IoT for work and life

☐

Handling personal information: At first, it is a threat to acquire information about people, such as people, cars, biological information about people, etc. reflected in a camera.

☐

Sending personal information: resisting sending your own location information

☐

Secondary use of data: the data you intentionally provided will be used for unexpected purposes

☐

Data leakage: information is filtered from the information service to the outside.

☐

Data alteration. You can't rely on whether the data measured by the IoT device is true or not.

☐

Data Ownership: the ownership of the data you intentionally provided is unclear.

☐

Data accuracy: it is impossible to know precisely the accuracy of the IoT device (sensor) that measured the data, the measurement environment, etc

☐

Intrusion into IoT devices: IoT devices are hijacked by attackers.

☐

Other:

If all of the above threats are resolved, would you like to use environmental measurements in the regional IoT (to present it as a local government, to use data as a citizen or company for everyday life, etc.)?

I don't want to take advantage of it at all.

1

2

3

4

5

I want to use it actively

If data security and privacy were not a barrier, would you be willing to use connected devices in order to improve your quality of life?

☐

Only those devices that collect data on my well-being

☐

Only those devices that collect data from the home

☐

Only those devices that collect environmental data from the city

☐

I would be willing to use all kinds of devices that would help me improve my quality of life.

☐

I would not like to use any type of device connected to each other

BACK

NEXT

Page 3 of 4

Figure 25. Use Case 1 Survey Step 3





Evaluation of functionalities

Have you ever take part of previous EU project pilots in the city of Santander?

☐ Yes

☐ No

☐ Maybe. I'm not totally sure

If yes, could you specify which and how?

Your answer

Indicate how you would rate the following functionalities between 1 and 5, where 1 is "unimportant" and 5 is "very important". *

	1	2	3	4	5	N/A
Check environmental data (temperature, humidity) in real time	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Know noise level in real time	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Generate heat maps of certain spots in the city	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Browse past environmental information	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Report abnormal values in environmental information in real time.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Periodically notify the information of the environment of a specific place.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Analyze in combination with environmental and other information such as public affluence	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Publish data measured by an individual.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Additional feedback. Which functionalities would you like to have? *

Your answer

Any additional comments regarding this use case?

Your answer

Name (optional)

Your answer

Figure 26: Use Case 1 Survey Step 4



Use Case 2 Survey

Horizon 2020, M-Sec, Wellbeing and Health use case in an active and independent society

Horizon 2020 is the largest research and innovation program in the European Union with a budget of almost 80 billion € for the period 2014-2020. Its main objective is to ensure the global competitiveness of Europe by financing research and development activities. It is open to the participation of research centres, universities or companies from any country in the world.

Within this innovation program, there is the "M-Sec" project formed by a consortium of twelve partners (six European and six Japanese), which began last July and will be developed over a period of 36 months. The main objective is to create a platform using the most advanced current technologies, to ensure the integrity and confidentiality of all data / information collected through the Internet of Things (all those devices connected together capable of collecting and exchanging data, for example, appliances, lights, thermostats, air quality sensors, humidity, smoke detection, smart watches or bracelets, etc.).

One of the pilots that is being worked on and which will be developed in the city of Santander, is related to the increase in life expectancy and, consequently, the increase in the number of elderly people year after year. Many cities are considering the challenge of improving the quality of life of their citizens through a solution that allows measuring a series of parameters of well-being and home through intelligent and connected devices, such as presence sensors (device to monitor some irregular habit such as that the refrigerator has not been opened for more than two days in a row), smoke sensors, electronic pillbox (message reminding the user that he or she has to take the medication), pedometer, wristband or watch to measure the quality of sleep , etc. . Other functionalities that are intended to be provided, is to make available to users a tool that allows them to communicate with their caregiver, family member, friends at any time.

Provided information

Your personal data and statements provided will be evaluated in strict confidence and processed anonymously. In case you do not feel comfortable answering a question; you have the possibility to reject the question. Also, at any time during the survey you have the possibility to finalize it. This decision will have no consequence for you.





Respondent profile

- Age ☐ 50-60 ☐ 61-70 ☐ 71-80 ☐ +81
- Live with: ☐ Alone ☐ Children ☐ Couple ☐ Couple and Children
- ☐ Other (Please, specify)

Technological knowledge

1.- What is your technological experience?

- ☐ Very high
- ⇒ I use several devices daily to access the internet
 - ⇒ I use applications such as email, WhatsApp, social networks, etc.
- ☐ High
- ⇒ I use a single device to access the internet daily
- ☐ Medium
- ⇒ I have a computer or tablet or mobile phone and I use it sometimes
- ☐ Low
- ⇒ I have a computer or tablet or mobile phone but it is unusual for me to use it.
 - ⇒ I do not think I should use it to a greater extent
- ☐ Very low
- ⇒ I do not have a computer / Tablet / mobile or internet
 - ⇒ I have never or rarely used technological devices

2.-What attitude do you have about the use of technologies?

- ☐ Positive: I would like to try new devices or technologies
- ☐ Neutral: I do not know or I do not care
- ☐ Negative: I do not like technology and I try to take it away from me.

3.- What devices do you use?

- ☐ Computer ☐ Phone ☐ Tablet ☐ Smart watch ☐ MP3/MP4





☐ Other (Please, specify)

4.- What kind of searches / activities have you done in the last 30 days from your computer, mobile or tablet?

☐ Mail box

☐ News

☐ Sports

☐ Shopping

☐ Recipes

☐ Activities

☐ Other: _____

☐ Chat (Ej. WhatsApp)

☐ Weather

☐ Bank

☐ Games

☐ Health and Wellbeing information

☐ Transport

☐ I have not done any activity because I have not a computer, mobile or tablet.

Security, privacy and use

5.- What worries you the most about the use of technological devices?

☐ Theft of personal data ☐ Use of your data for other purposes ☐ Mistrust in the results of the measured parameters ☐ Ownership of the data ☐ Difficulty in the use of devices

☐ Other (Please, specify)

6.- If the security and privacy of data was not a barrier, would you be willing to use connected devices, (smoke sensor, electronic pillbox, presence sensor, bracelet to measure sleep quality) in order to improve its quality of life?

☐ Only those devices that collect data on my well-being

☐ Only those devices that collect data from home

☐

☐



I would be willing to use all kinds of devices that will help me improve my quality of life

I would not like to use any type of IoT device

7.- Would you like to be able to share the data collected with your relatives or caregivers?

☐ Yes

☐ No

Valoración funcionalidades

8.- Mark with a circle how you would evaluate the following functionalities between 1 and 5, where 1 is "not important" and 5 is "very important"

Have a SOS button to ask for help at any time	1	2	3	4	5
Use an electronic pillbox that allows to generate alarms when the medicine has not been taken	1	2	3	4	5
Have a presence sensor to control an irregular habit (Ex: Not having opened the refrigerator for more than 2 days in a row, may indicate that something has happened to the user).	1	2	3	4	5
Have a smoke detector (CO2)	1	2	3	4	5
Have a humidity detector	1	2	3	4	5
Having a window sensor, allows to control if the window is open or closed	1	2	3	4	5
Have a water leak detector	1	2	3	4	5
Have a fall detector	1	2	3	4	5
Have a wristband / watch that measures the quality of sleep based on the hours you have slept, the times you	1	2	3	4	5





have woken up, the minutes of deep or light sleep.

Have a pedometer to monitor daily physical activity	1	2	3	4	5
Have an electrical sensor to control the power consumption of a particular device	1	2	3	4	5
Have a communication channel that can be used to connect with family, friends, caregivers in an easy and simple way (send photos, make video calls, chat)	1	2	3	4	5
Have an automatic notification that allows to know your wellbeing status and therefore make it known to your relatives or caregivers	1	2	3	4	5
Learn about activities that take place in your city	1	2	3	4	5
Register in a simple way in these activities	1	2	3	4	5
Learning about care and wellbeing	1	2	3	4	5
Learning about preventive health	1	2	3	4	5
Create a user profile	1	2	3	4	5
To be able to communicate with other users of the application	1	2	3	4	5
Create groups to talk with other users	1	2	3	4	5

Thank you very much for your kindness and for the time spent answering this survey





Use Cases 3, 4 & 5 Surveys (originally in Japanese)

EU-JP collaboration project "M-Sec" stakeholder questionnaire (use case 3, 4, 5)

We will assume that "sensors" and small computers are mounted on various items used in municipality-related tasks to "make it IoT". For example, suppose you install a computer and a sensor in a public vehicle and measure environmental information such as pollen volume in the air and PM 2.5 concentration, or monitor the degradation condition of the road with a camera. By doing this, it seems that you can comprehensively observe the whole area with few sensors. Also, administrative officials and citizens themselves send measured environmental information to the cloud service, or post pictures of problem events (road holes, illegal dumps, etc.), observations that the machine does not know. It seems likely. I will call IoT covering the whole area like this "regional IoT".

Meanwhile, recently attacks against IoT devices such as surveillance cameras and microcomputers are rapidly increasing, and a large number of them have been left in a state of being "hijacked". Some surveillance camera images are leaked on the Internet. Also, in sensing by staff and citizens themselves, it is necessary to send location information and photos, so personal information of those people will be included in the collected data.

The use case 3 of the Japan-Europe collaboration project "M - Sec" aims to collect environmental information data well and use it for the municipality business while coping with such threats. In addition, use case 4 aims to safely collect information related to individuals and areas (information on home garbage emissions and specific spots) and use it for smart areas. Use case 5 creates a mechanism that combines these to make the city fun.

Based on the above, please answer the following questions.

Age						
<input type="checkbox"/> 15 - 30						
<input type="checkbox"/> 31 - 45						
<input type="checkbox"/> 46 - 60						
<input type="checkbox"/> 61 - 75						
<input type="checkbox"/> 76+						
Please tell us your position at the time of reply *						
<input type="checkbox"/> I am answering as a municipal official						
<input type="checkbox"/> I am answering as a local resident						
<input type="checkbox"/> I am answering as a staff of a private company						
<input type="checkbox"/> I am answering as an official of NPO group etc.						
<input type="checkbox"/> I am answering as a researcher of a university, a research institute, etc.						
<input type="checkbox"/> Other						





Please tell us about your experience with information technology.								
<input type="checkbox"/>	I have an extremely high level of experience - access the internet everyday with multiple devices. We frequently use e-mail, SNS, web service and so on.							
<input type="checkbox"/>	Have advanced experience - Access the Internet almost every day using one device.							
<input type="checkbox"/>	Somewhat experienced - I own a computer or tablet and access the Internet around 2 to 4 days per week.							
<input type="checkbox"/>	I do not have much experience - I own a computer or tablet, but I use it about once or less per week.							
<input type="checkbox"/>	I have no experience at all - I do not own a computer or tablet.							
Please tell us your thoughts on information technology. *								
<input type="checkbox"/>	Positive - I would like to try new technologies and new equipment in business and everyday life.							
<input type="checkbox"/>	Negative - I would like to avoid new technologies and new equipment in business and everyday life.							
<input type="checkbox"/>	I do not know either or neither.							
Please tell me the equipment you have. *								
<input type="checkbox"/>	Desktop Computer							
<input type="checkbox"/>	Notebook Computer							
<input type="checkbox"/>	Smart phone							
<input type="checkbox"/>	Tablet Computer							
<input type="checkbox"/>	Smart watch							



Please tell us what you feel as a threat in introducing IoT for work and life *	
<input type="checkbox"/>	Data leakage - Information leaks from the information service to the outside
<input type="checkbox"/>	Intrusion into IoT devices - IoT devices are hijacked by attackers
<input type="checkbox"/>	Handling of personal information It is a threat in the beginning to acquire information on individuals, such as people, cars, biological information of people, etc. reflected in a camera camera
<input type="checkbox"/>	Sending personal information - resisting to sending your own location information
<input type="checkbox"/>	Handling of spot information - It is a threat in the beginning to acquire information on a limited space (spot) such as a person or a car reflected on the camera at a specific place
<input type="checkbox"/>	Intrusion into the cloud system - Cloud systems that process data measured on IoT devices are hijacked by attackers
<input type="checkbox"/>	Secondary use of data - Data you intentionally provided will be used for unexpected purposes
<input type="checkbox"/>	Data alteration It can not be trusted whether the data measured by the IoT device is true or not
<input type="checkbox"/>	Data accuracy - It is impossible to accurately know the accuracy of the IoT device (sensor) that measured data, measurement environment, etc.
<input type="checkbox"/>	Ownership of data - ownership of data you intentionally provided is unclear
<input type="checkbox"/>	Other:





If all of the threats mentioned above are resolved, would you like to utilize environmental measurements introduced by a local government, to utilize data as a citizen or company for daily life etc)? *

	I do not want to take advantage of it at all				I want to actively use it	
	1	2	3	4	5	
Please rate each of the following features of regional IoT.						
	I do not want to take advantage of it at all				I want to actively use it	
Environment information related function						
	1	2	3	4	5	Determine environmental information finely (eg every 1 meter square)
	1	2	3	4	5	Grasp the environmental information roughly (for example, by district)
	1	2	3	4	5	Understand environmental information in real time
	1	2	3	4	5	Examine past environmental information
	1	2	3	4	5	Analyze in combination with environmental information and other information
	1	2	3	4	5	Notify abnormal value in environmental information in real time
	1	2	3	4	5	Periodically notify environment information of a specific place
	1	2	3	4	5	Post data measured by an individual





Cleaning work related function						
	1	2	3	4	5	Determine the amount of garbage discharge finely (eg for each family)
	1	2	3	4	5	Grasp garbage discharge amount roughly (for each district etc.)
	1	2	3	4	5	Understand garbage collection amount in real time
	1	2	3	4	5	Determine past emissions
	1	2	3	4	5	Analyze in combination with waste emissions and other information
	1	2	3	4	5	Notify abnormal value of dust discharge amount in real time
	1	2	3	4	5	Regularly notify the amount of dust emission at a specific place



Spot related function						
	1	2	3	4	5	Determine spot information finely (eg every 1 meter square)
	1	2	3	4	5	Grasp spot information roughly (for example, by district)
	1	2	3	4	5	Understand spot information in real time
	1	2	3	4	5	Examine past spot information
	1	2	3	4	5	Analyze in combination with spot information and other information
	1	2	3	4	5	Notify abnormal value in spot information in real time
	1	2	3	4	5	Periodically notify spot information of a specific place
	1	2	3	4	5	Post data measured by an individual





Use Case 6 Survey

M-Sec Use Case 6

Horizon 2020 is the largest research and innovation programme in the European Union with a budget of almost €80 billion for the period 2014-2020. Its main objective is to ensure Europe's global competitiveness by funding research and development activities. It is open to the participation of research centres, universities or companies from any country in the world.

Within this innovation programme is the "M-Sec" project formed by a consortium of twelve partners (six European and six Japanese), which began last July and will run for 36 months. The main objective is to create a platform using the most advanced current technologies, to guarantee and ensure the integrity and confidentiality of all data/information collected through the Internet of Things (all those devices connected to each other capable of collecting and exchanging data, for example, appliances, lights, thermostats, air quality sensors, humidity, smoke detection, watches or intelligent wristbands, etc.).

One of the pilot tests in the city of Santander will seek to give a new impetus to the citizen participation tool known as "Pulse of the city", through which municipal services can be notified of the need for potential actions where indicated by the user of the app.

* Required

Email address *

Thanks for your participation!



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

Figure 27: Use Case 6 Survey Introduction





Participant profile - Age *

☐ 15-30

☐ 31-45

☐ 46-60

☐ 61-75

☐ +76

Participant occupation

☐ Municipal official

☐ Local resident

☐ Staffer of a private company

☐ Researcher at the University or a research center

☐ Other: _____

[NEXT](#)

Page 1 of 4

Never submit passwords through Google Forms.

Figure 28: Use Case 6 Survey Step 1





Technological skills

What is your technological experience? *

☐ Very high - I use several devices daily to access the internet. I use applications such as e-mail, WhatsApp, Social networks

☐ High - I use a single device to access the internet on a daily basis

☐ Medium - I have a computer or tablet or mobile and use it sometimes

☐ Low - I have a computer or tablet or mobile but it is rare that I use it.

☐ Very low - I don't have a computer/Tablet/mobile or internet

What is your attitude towards the use of technologies?

☐ Positive: I would like to try new devices or technologies

☐ Neutral: I don't know or don't care

☐ Negative: I don't like technology and try to take it away from me.

What devices do you use?

☐ Personal Computer

☐ Laptop

☐ Mobile phone

☐ Tablet

☐ Smart watch

☐ MP3/MP4

What kind of searches/activities have you carried out in the last 30 days from your computer, mobile or tablet?

☐ E-mail

☐ News

☐ Sports

☐ Shopping

☐ Cooking

☐ Leisure

☐ Chat

☐ Weather

☐ Banking

☐ Gaming

☐ Transportation

☐ I haven't done anything because I don't have a computer, mobile phone or tablet.

BACKNEXTPage 2 of 4

Figure 29: Use Case 6 Survey Step 2



Security & Privacy

What worries you most about the use of technological devices?

- ☐ Handling personal information: At first, it is a threat to acquire information about people, such as people, cars, biological information about people, etc. reflected in a camera.
- ☐ Sending personal information: resisting sending your own location information
- ☐ Secondary use of data: the data you intentionally provided will be used for unexpected purposes
- ☐ Data leakage: information is filtered from the information service to the outside.
- ☐ Data alteration. You can't rely on whether the data measured by the IoT device is true or not.
- ☐ Data Ownership: the ownership of the data you intentionally provided is unclear.
- ☐ Data accuracy: it is impossible to know precisely the accuracy of the IoT device (sensor) that measured the data, the measurement environment, etc
- ☐ Intrusion into IoT devices: IoT devices are hijacked by attackers.
- ☐ Other: _____

If all the threats mentioned above are resolved, would you like to participate in the daily management of your city by sending personalized reports (anomalous situations, malfunctions)?

	1	2	3	4	5	
I don't want to participate at all.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	I want to use it actively

If data security and privacy were not a barrier, would you be willing to use this kind of online application in order to improve your city?

- ☐ I would be willing to use all kinds of devices that would help me improve my quality of life.
- ☐ I would not like to use any type of device connected to each other
- ☐ Other: _____

BACK

NEXT

Page 3 of 4

Never submit passwords through Google Forms.

Figure 30: Use Case 6 Survey Step 3





Evaluation of functionalities

Have you ever take part of previous EU project pilots in the city of Santander?

- ☐ Yes
- ☐ No
- ☐ Maybe. I'm not totally sure

If yes, could you specify which and how?

Your answer

Indicate how you would rate the following functionalities between 1 and 5, where 1 is "unimportant" and 5 is "very important". *

	1	2	3	4	5	N/A
Send incidents to municipal services via app	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Track incidents resolution via app	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Include images in the incident description	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Receive updates related to reported incidents	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Check and participate in other cities' reporting	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Additional feedback. Which functionalities would you like to have? *

Your answer

Any additional comments regarding this use case?

Your answer

Name (optional)

Your answer

Figure 31: Use Case 6 Survey Step 4

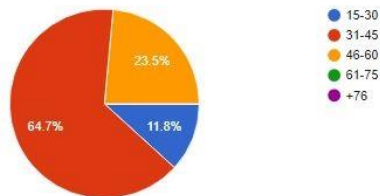


Annex 2 – Stakeholders Surveys results

Taking as an example a couple of surveys distributed among Santander citizens, in this case the ones related to Use Cases 1 and 6 where up to 20 people participated, the participation results let the consortium depict the profile of the future user of the solutions developed within the project.

First, the survey sketches a rough personal profile of the users, revealing they are quite young, among 31 and 45 years old, and they are providing their views as local residents or staffers of a private company. Figure 32 below shows this piece of information.

Participant profile - Age



Participant occupation

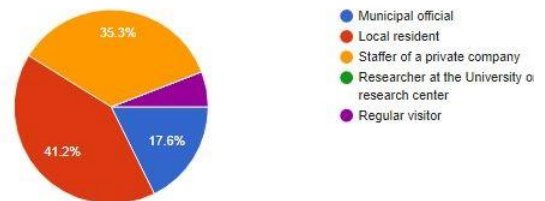
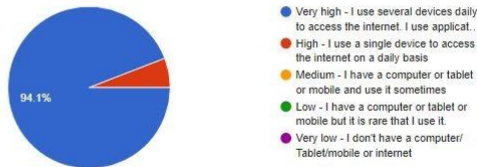


Figure 32: Survey – Participant profile

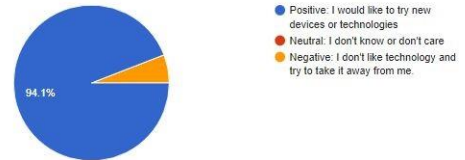
Probably related to this context the following piece of information, as shown in Figure 33, makes perfect sense, since they claim to have a high level of technological experience and demonstrate a propensity to know and use new technologies. In their daily routines they use mainly the mobile phone, closely followed by laptops, getting access to the Internet and using it principally to read the news and also check their e-mails and maintain conversations via chat applications.



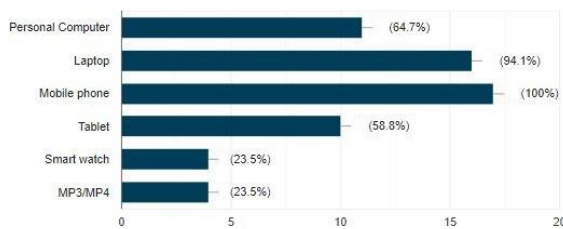
What is your technological experience?



What is your attitude towards the use of technologies?



What devices do you use?



What kind of searches/activities have you carried out in the last 30 days from your computer, mobile or tablet?

17 responses

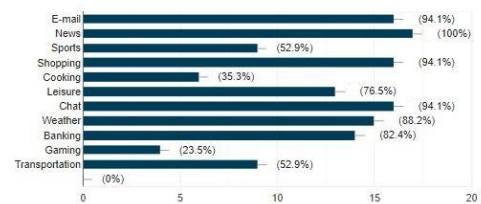
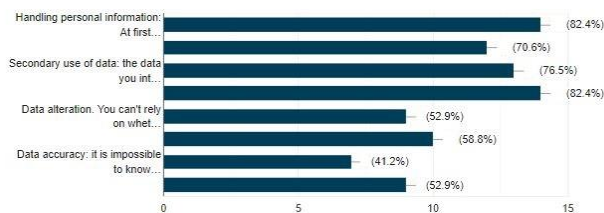


Figure 33: Survey - Technology and devices

Immersed in this context of high technological knowledge, their greatest concern when working in IoT environments, as shown in Figure 34, relates to the handling of personal data, as well as possible unwanted leaks. In any case, they are willing to use any type of device that helps to improve their day-to-day life.

Tell us what you feel is a threat by introducing IoT for work and life

17 responses



If data security and privacy were not a barrier, would you be willing to use connected devices in order to improve your quality of life?

17 responses

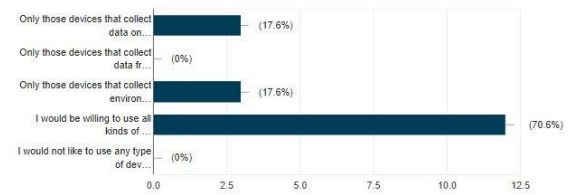


Figure 34: Survey - Threats and willingness

Finally, and as a possible yardstick to measure whether it will be possible to count on citizen participation during the pilot experiences to be developed as part of M-Sec, it is requested to specify whether it has taken part in the trials of other European projects carried out in Santander. The answers in this case are not entirely conclusive, as can be seen in Figure 35, although almost half of those surveyed admit that they did not participate actively in them.



Have you ever take part of previous EU project pilots in the city of Santander?

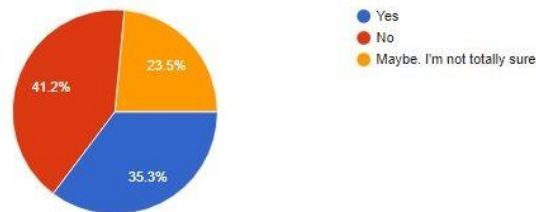


Figure 35: Survey - Previous participations

Every survey adapts to the specifics of both European and Japanese audience and can be fully checked in the Annexes of this report.

Regarding Use Case 2, several meetings were organized with different municipal services that deal with elderly people, as they know them the best, with the aim of reaching the greatest number of users. During these meetings, this survey was discussed. On the one hand, the social services department together with the service concession company raised the low technological profile of users of the telecare service, due to their advanced age and physical conditions, as well as their reluctance to interact with new technologies. On the other hand, managers of civic centres commented on the different activities aimed at the elderly that are organized in the city, such as memory workshops, gymnastics, yoga, etc. where most of the attendees are familiar with new technologies (they have a smartphone).

Despite the existing technology gap, the survey has been distributed among a small group, the users of the telecare service and among attendees of the civic centres activities.

In the case of telecare users, 14 people have accepted to respond the survey. The majority of respondents are older than 81 years old and they live alone, as can be seen in the next Figure 36.

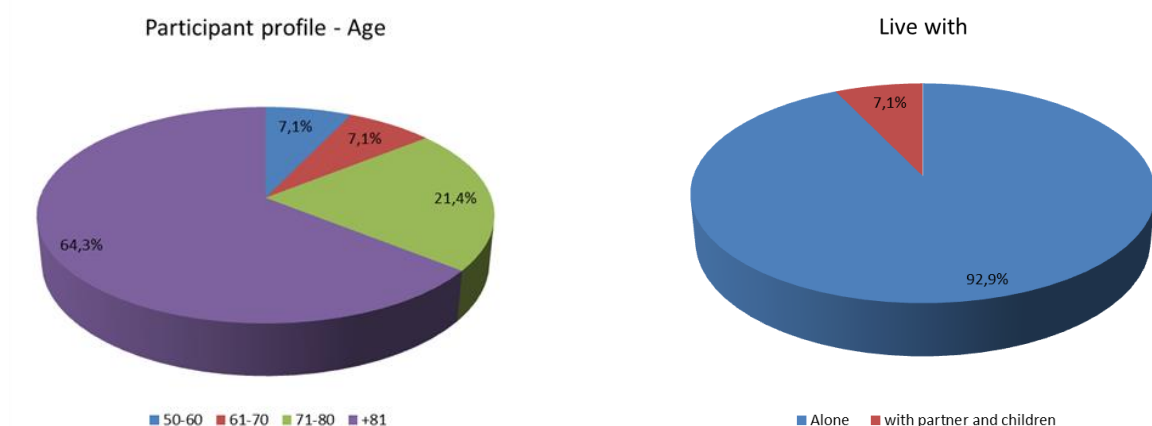


Figure 36: Telecare Survey – Participant profile



Regarding their technological experience, half of those surveyed consider that they have a very high level and a positive attitude about the use of new technologies, whereas almost 35% consider their level to be low or very low, as can be seen in the following figures. Going deeper into the type of devices they usually use and also the activities carried out, although most of them have a mobile phone, only half of them use chat applications, while more than 40% admit that they have not carried out any kind of search or activity in the last month because they do not have any device. These can be seen in the following Figure 37. Analysing the type of devices they use and the activities they carry out, we would consider they have a low technological level, which does not fit with their perception, as it can be seen in the survey results. However, it is important to take into account the respondent's profile: most of them are people older than 81 years used to using a fixed telephone and for whom using a mobile phone can be quite complicated, so they value it very much.

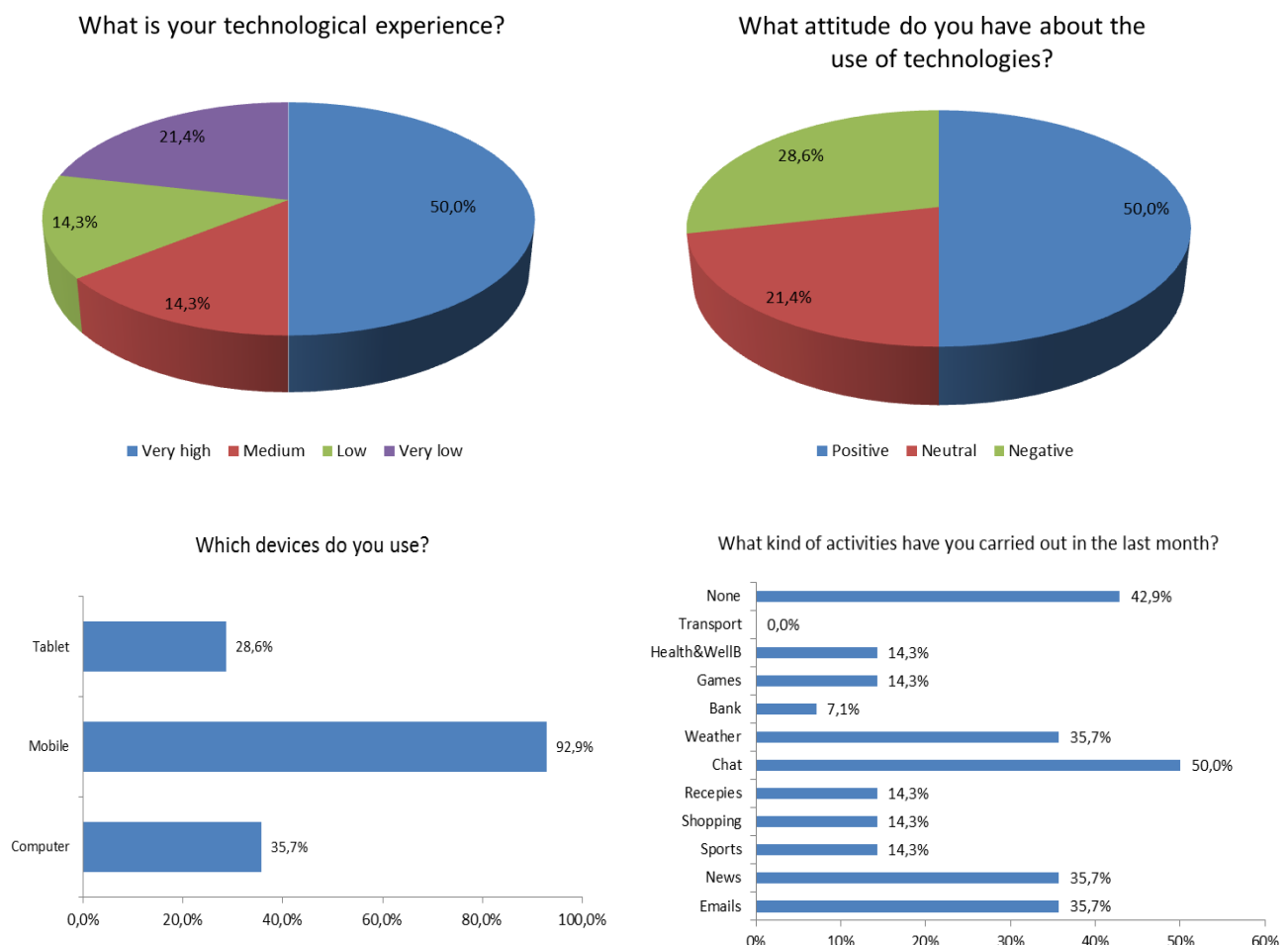


Figure 37: Telecare Survey – Technology and devices

Their main concern about using technological devices is related to the difficulty in the use of the devices, followed by the theft of personal data. This result fits with the fact that regardless of ensuring privacy, most of them would not use connected devices, as can be seen in the next Figure 38. On the other hand, more



than 20% of them would use home devices to improve their quality of life. Additionally, a small percentage of respondents would be willing to share their data with their relatives or caregivers.

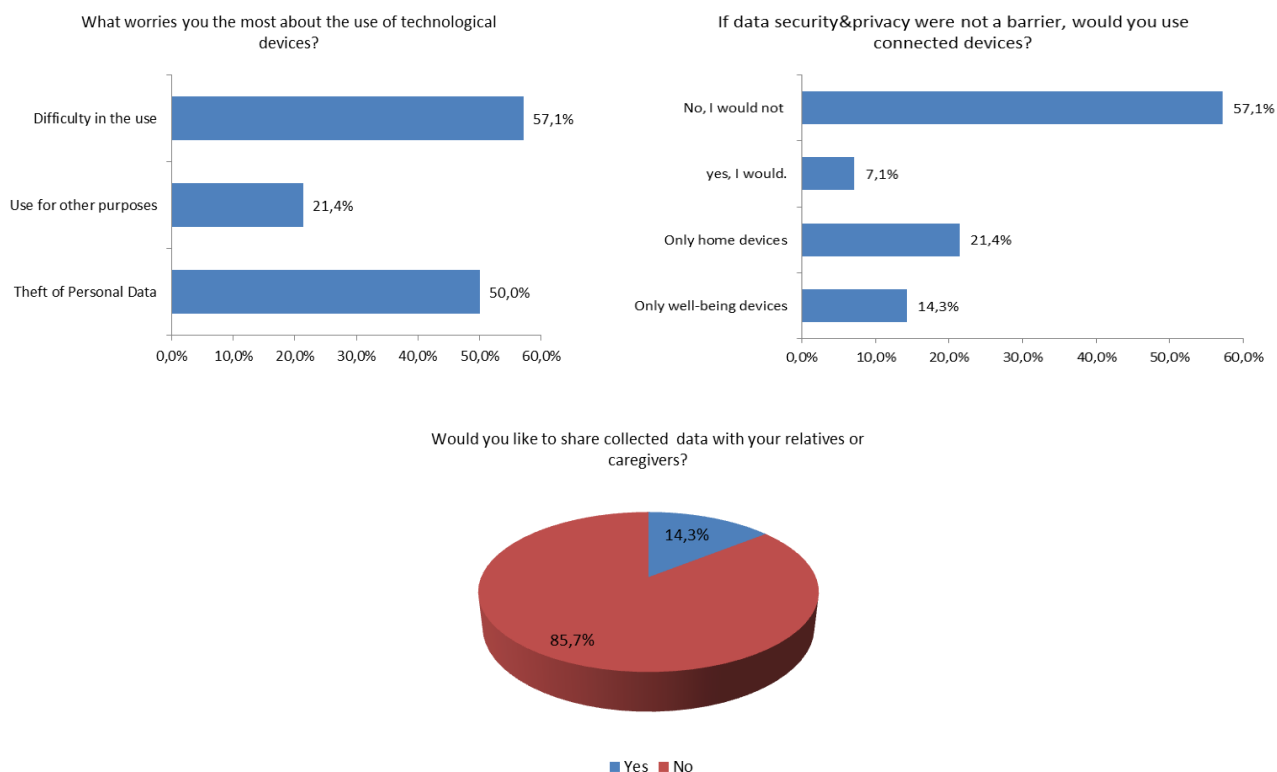


Figure 38: Telecare Survey – Security & privacy

Finally, we wanted to know what functionalities would be more attractive and useful to them. As can be seen in the next Figure 39, the most interesting ones are those related to home devices such as SOS button, smoke detector, or fall detector, which are the ones that are currently included within the telecare service. However, the least interesting ones are those related to the use of applications, such as *“create a profile”* or *“receive automatic notifications”*.



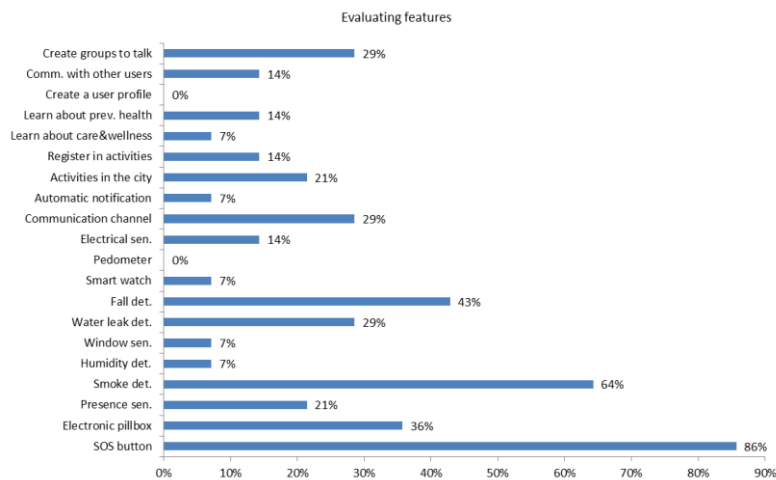


Figure 39: Telecare Survey – Evaluating features

As a conclusion, a small group of telecare users could improve their quality of life through the use of new technological solutions as long as they do not need to interact with them.

In the case of the attendees of the civic centres activities, the majority of the 60 survey respondents are older than 71 years and their personal situation is quite varied, being living with a partner and living alone the most significant ones, as can be seen in the following Figure 40.

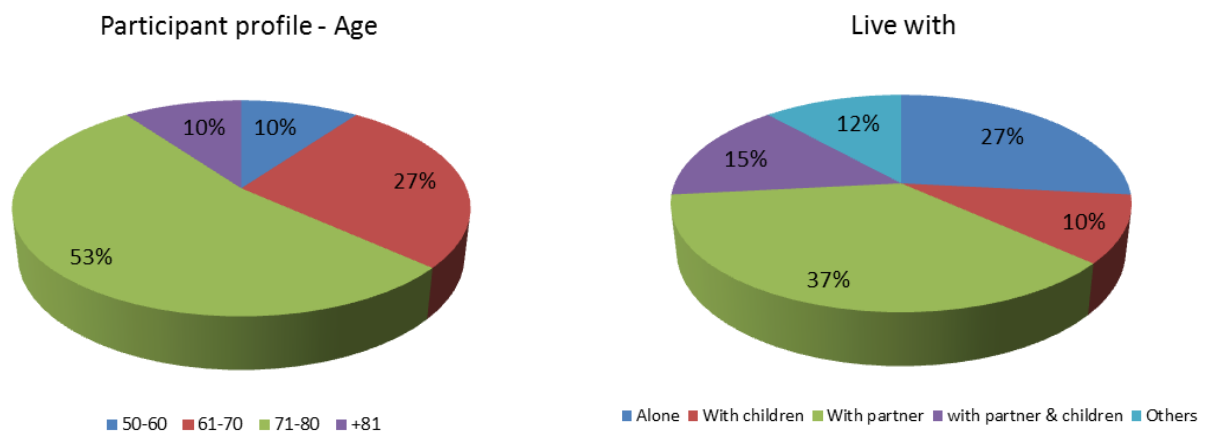


Figure 40: Civic centres Survey – Participant profile

In terms of their technological experience, almost half of those surveyed consider that they have a low or very low level, while 38% consider that their level is medium. However, most of them have a positive attitude about the use of technologies. Analysing in more detail their technological profile we discovered that more than 80% of them use mobile phone and almost 30% computer and tablet for different activities such as reading the news, checking weather forecast or using chat applications. Although they think their technological level is low, they use new technologies frequently (see Figure 41).

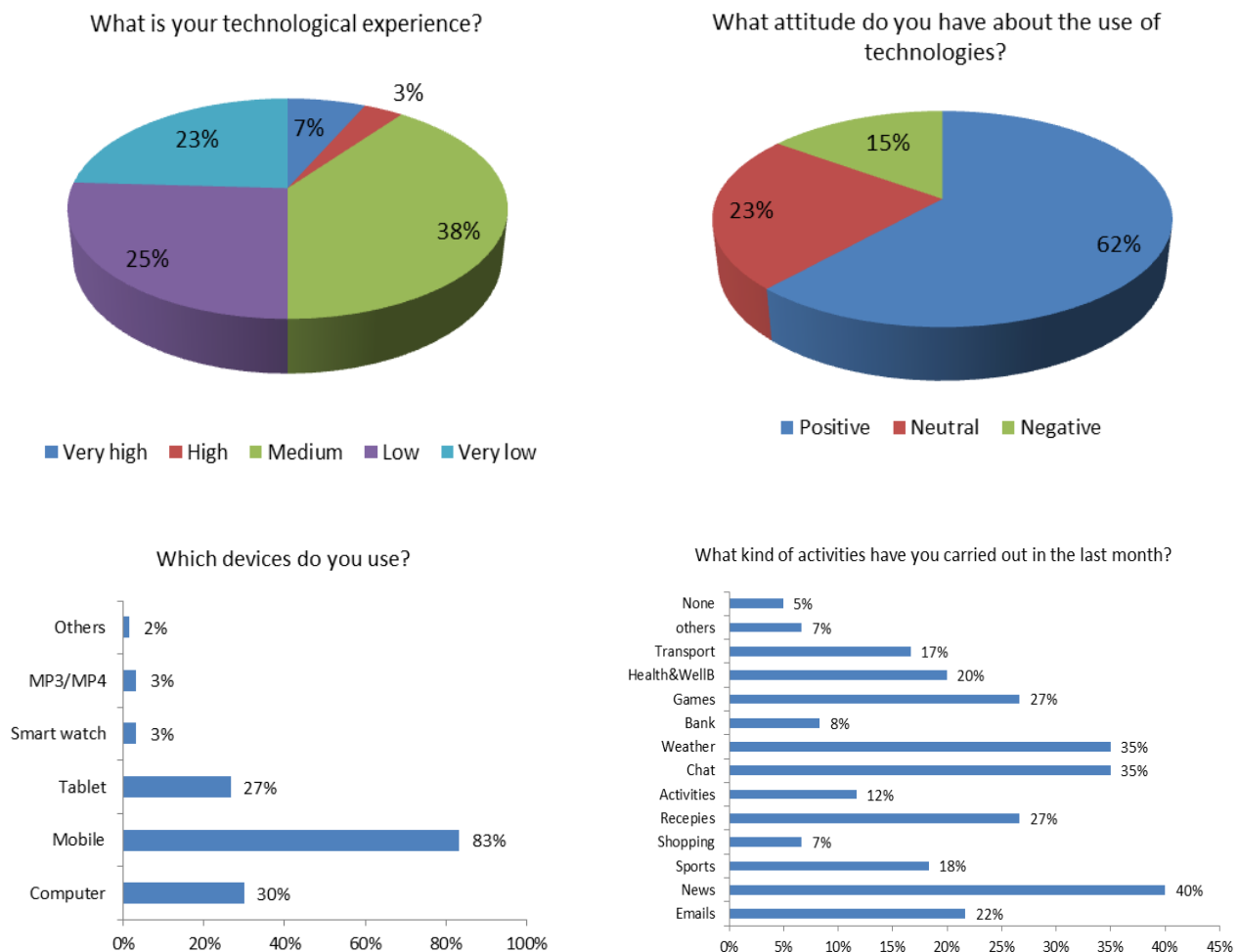


Figure 41: Civic centres Survey – Technology and devices

Their greatest concern about using technological devices, as can be seen in the next Figure 42, relates to the use of data for other purposes and also theft of personal data. In spite of that, they are willing to use devices that help them to improve their quality of life, having more interest in wellbeing devices than in home devices. Additionally, they would be in favour of sharing collected data with their relatives.



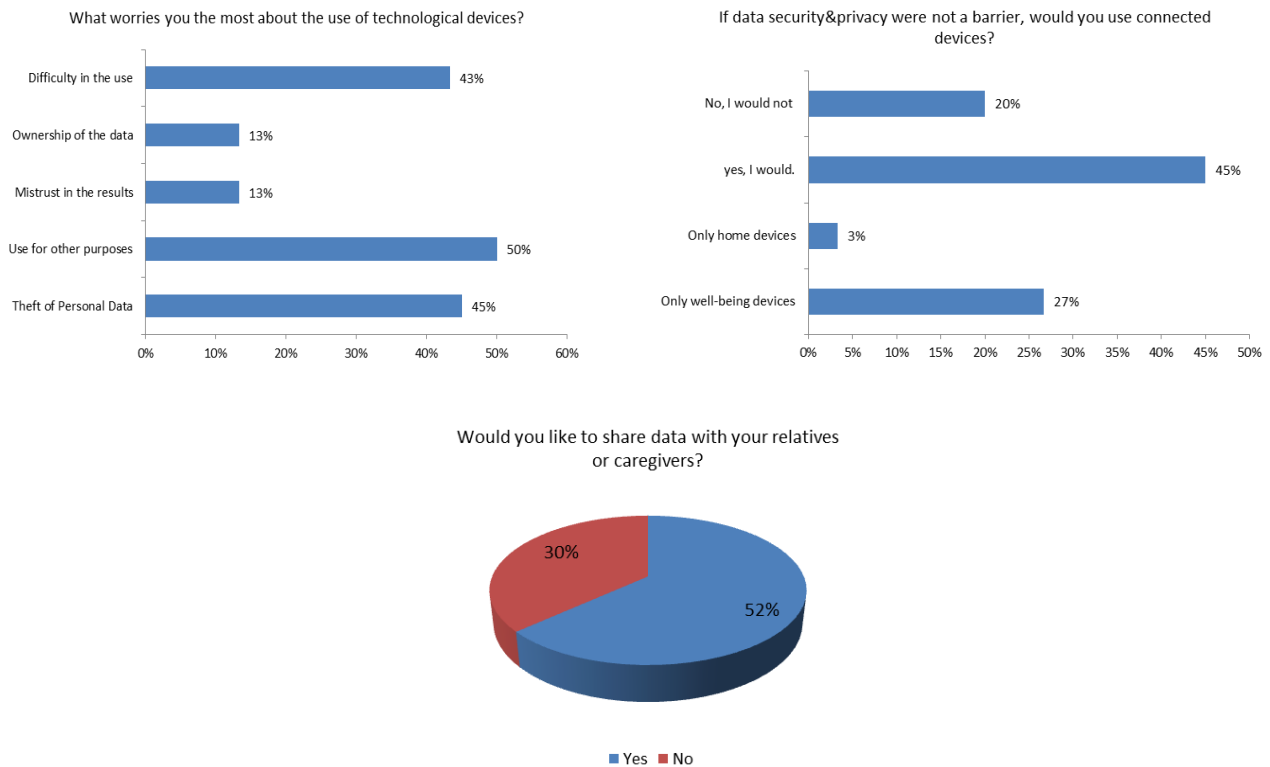


Figure 42: Civic centres Survey – Security & Privacy

Finally, the following Figure 43 shows their assessment of the proposed functionalities. As in the case of users of telecare service, the most interesting features are those related to home devices such as SOS button, smoke detector, or fall detector, however, they are also quite interested in being informed and registering for organized activities in the city, learning about care and wellness...

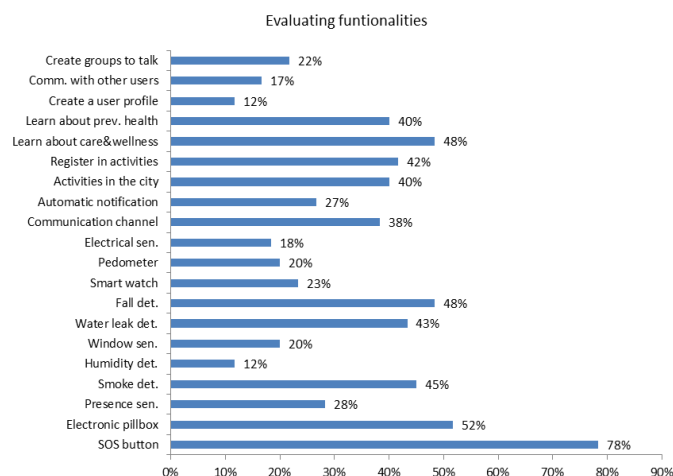


Figure 43: Civic centres Survey – Evaluating features





As summary, attendees of the civic centre activities in Santander have not only a good technological profile but also a positive attitude to interact with new technologies to improve their quality of life.

Regarding Use Cases 3, 4, and 5, a questionnaire survey was conducted for 49 persons. The major purpose of this survey is to illustrate (1) their demand to IoT technology in terms of environmental sensing (Use Case 3), citizens care (Use Case 4) and marketplace (Use Case 5), and (2) their thoughts on threats in leveraging them. First, the survey sketches a rough personal profile of the users, revealing they are quite young. Almost 75% of them are 15-45 years old, and half of them are providing their views as municipal officials. 21% and 14% of them are local residents and researchers, respectively. The following graphs in Figure 44 show this piece of information.

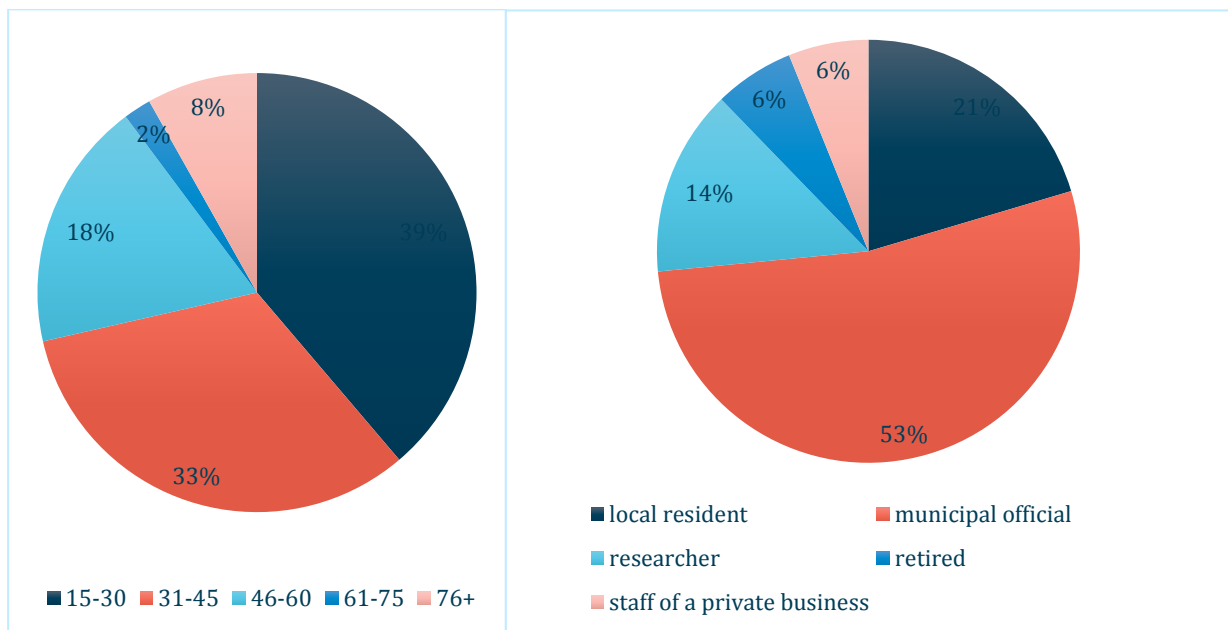


Figure 44: Survey – Participants profile (Use Cases 3, 4, 5)

This naturally corresponds to the following results shown in Figure 45, where most of them say they have advanced experience on the use of information technology. Only 2% say they do not have much experience. Perfectly matching this is the participant's attitude to information technology. Almost 90% of them are positive against technology, saying "I would like to try new technologies and new equipment in business and everyday life." Though some participants are negative on information technology, or not accustomed to it, the list of devices they own (Table 11) clarifies that they live with the technology. Therefore this survey is meaningful in knowing their feeling to the technology itself, threats it causes, and its use for making cities smarter.

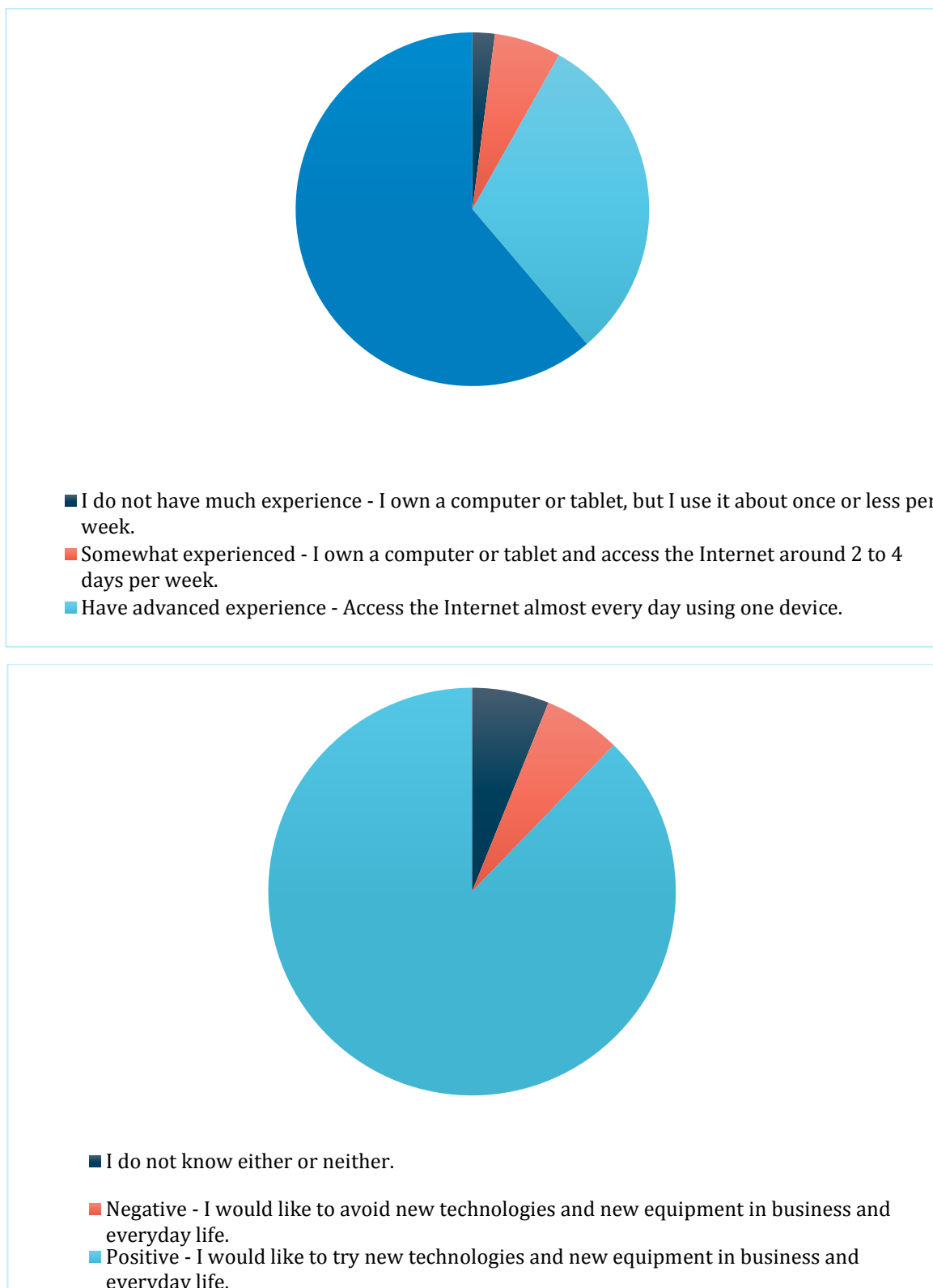


Figure 45: Survey – Participants Experience (above) and Attitude (below) to Information Technology





Table 11: Devices owned by the participants

Desktop PC	1
Desktop PC;Notebook PC	5
Desktop PC;Notebook PC;Smartphone (Android)	1
Desktop PC;Notebook PC;Smartphone (iPhone);Smartphone (Android);Smart Watch	1
Desktop PC;Notebook PC;Smartphone (iPhone);Smartphone (Android);Tablet	1
Desktop PC;Notebook PC;Smartphone (iPhone);Smartphone (Android);Tablet;AI Speaker	1
Desktop PC;Notebook PC;Smartphone (iPhone);Tablet	4
Desktop PC;Notebook PC;Smartphone (iPhone);Tablet;AI Speaker	1
Desktop PC;Notebook PC;Smartphone (iPhone);Tablet;Smart Watch	2
Desktop PC;Notebook PC;Smartphone (iPhone);Tablet;Smart Watch;AI Speaker	2
Desktop PC;Smartphone (Android)	1
Desktop PC;Smartphone (iPhone)	2
Desktop PC;Smartphone (iPhone);Tablet	2
Notebook PC	1
Notebook PC;Smartphone (Android)	1
Notebook PC;Smartphone (Android);Tablet	2
Notebook PC;Smartphone (iPhone)	6
Notebook PC;Smartphone (iPhone);AI Speaker	1
Notebook PC;Smartphone (iPhone);Smartphone (Android)	1
Notebook PC;Smartphone (iPhone);Smartphone (Android);Tablet;Smart Watch	1
Notebook PC;Smartphone (iPhone);Tablet	9
Notebook PC;Smartphone (iPhone);Tablet;Smart Watch	1
Notebook PC;Smartphone (iPhone);Tablet;Smart Watch;AI Speaker	2

The next piece of information reveals how they find the threats in use of information technology. Not surprisingly, data leakage is top-ranked (see Figure 46). This is considered natural since these years there were data leakage incidents in a few large private companies. Intrusions to IoT devices / cloud systems are also highly ranked. Another major concern is regarding personal information. In Japan, Personal Information Protection Law is becoming more and more a major brake for data-driven management in any domain including national government, regional government, industry, academia, etc. Opposingly, data accuracy is evaluated lower. In addition, secondary use of data, using data outside of the initial purpose, is relatively lower ranked. It can be inferred that data exchange through marketplace for better use of data would be feasible in some cases.

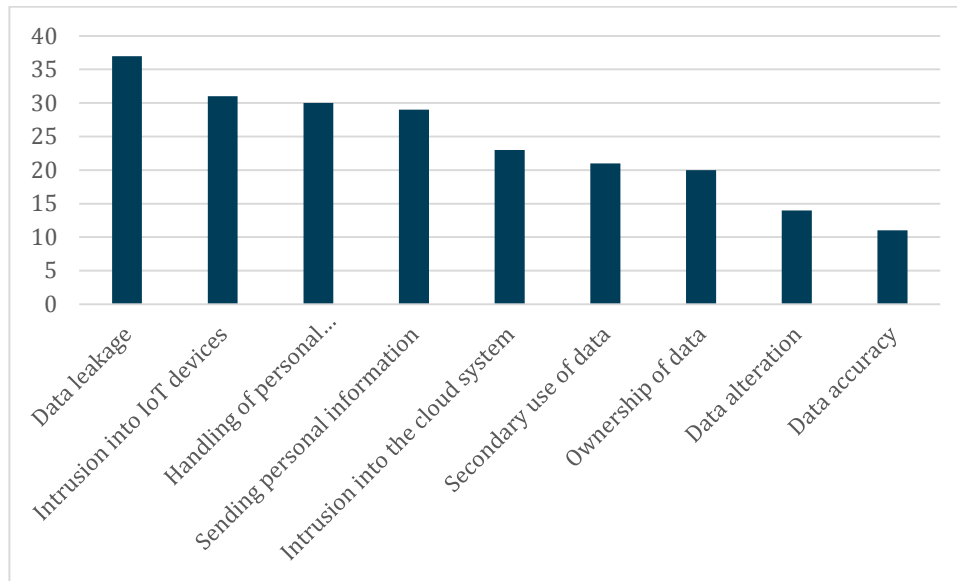


Figure 46: Survey – Threats in Use of Information Technology

The final survey evaluates participant's demand to the data on environment, local area and people. Figure 47 depicts the answers to "If all of the threats mentioned above are resolved, would you like to utilize environmental measurements in regional IoT (to introduce it as a local government, to utilize data as a citizen or company for daily life etc)?" Figure 48 shows the answers to "If all of the threats mentioned above are resolved, would you like to utilize "securely-collected data on the local area and people" in regional IoT (to introduce it as a local government, to utilize data as a citizen or company for daily life etc)?" These results show that there are concrete demands to IoT technology in terms of environmental sensing (Use Case 3), citizens care (Use Case 4) and marketplace (Use Case 5).

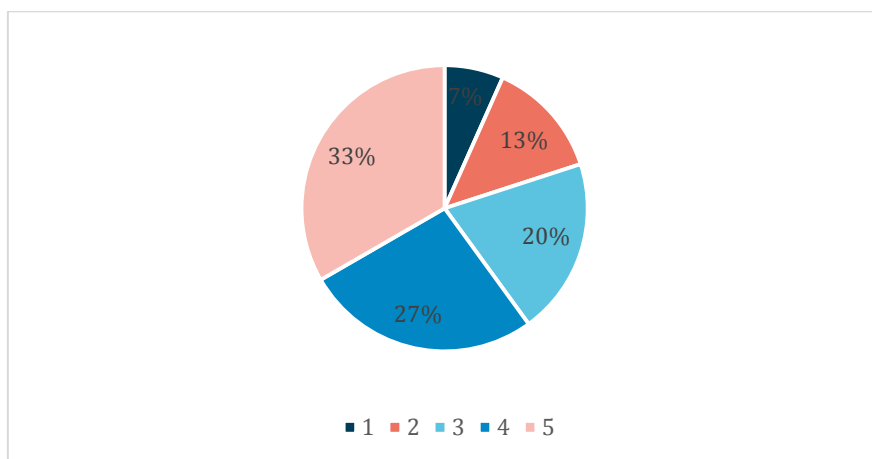


Figure 47: Survey – If all of the threats mentioned above are resolved, would you like to utilize environmental measurements in regional IoT (to introduce it as a local government, to utilize data as a citizen or company for daily life etc)?



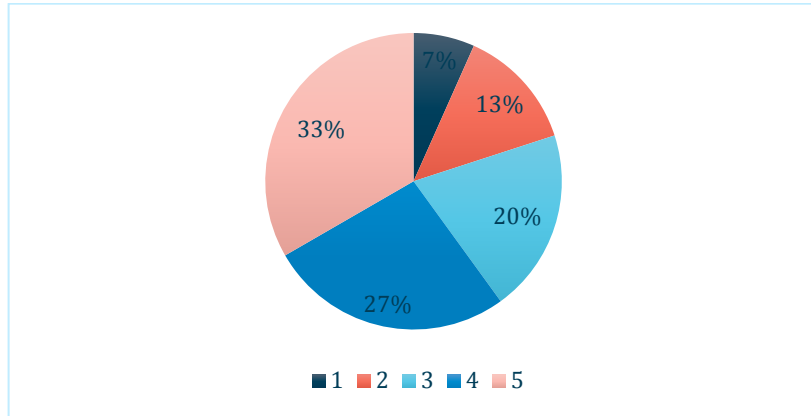


Figure 48: Survey – If all of the threats mentioned above are resolved, would you like to utilize "securely-collected data on the local area and people" in regional IoT (to introduce it as a local government, to utilize data as a citizen or company for daily life etc)?

