Multi-layered Security Technologies

for hyper-connected smart cities

D2.8: M-Sec validation and overall evaluation

October 2021

Grant Agreement No. 814917

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

Project acronym	M-Sec
Deliverable	D2.8 M-Sec validation and overall evaluation
Work Package	WP2
Submission date	October 2021
Deliverable lead	TST/WU
Authors	A. Puras (TST), N. Teles (F6S), A. Bokhari (YNU), V. Clemente (WLI), K. Doguchi (NTTE), A. Tsuge (KEIO), M. Gallissot (CEA), Sonia Sotero (AYTOSAN), O. Voutyras (ICCS), G. Palaiokrassas (ICCS)
Internal reviewer	O.Voutyras (ICCS), A. Tsuge (KEIO)
Dissemination Level	Public
Type of deliverable	R

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

Version history

#	Date	Authors (Organization)	Changes
v0.1	16 July 2021	Alberto Puras (TST)	ToC
v0.2	23 July 2021	Alberto Puras (TST)	New ToC
v0.3	16 August 2021	Alberto Puras (TST)	Final ToC
v0.4	16 September 2021	Vanessa Clemente (WLI)	Updated Section 2.3, 2.5 and 3.3
v0.5	20 September 2021	Alberto Puras (TST)	Updated Section 3.2
v0.6	20 September 2021	Nadine Teles (F6S)	Updated Section 3.1
v0.7	20 September 2021	Akira Tsuge (KEIO)	Merged first contribution in Section 3.4 and 3.5
v0.8	22 September 2021	Akira Tsuge (KEIO)	Merged missing part of 3.4
v0.9	22 September 2021	Aamir Bokhari (YNU)	Updated Section 2.2 & 3.4
v0.10	24 September 2021	Akira Tsuge (KEIO)	Updated according to review comment
v0.11	27 September 2021	Orfeas Voutyras (ICCS)	Updated Sections 2.1, 2.2, and 4.
v0.12	29 September 2021	Aamir Bokhari (YNU)	Corrected small errors in section 2.2 & 2.3
v0.13	29 September 2021	Vanessa Clemente (WLI)	Updated section 3.3
v0.14	30 September 2021	Alberto Puras (TST)	Updated Section 1
v0.15	30 September 2021	Vanessa Clemente (WLI)	Updated section 3.3
v0.16	30 September 2021	Alberto Puras (TST)	Added comments
v0.17	30 September 2021	Alberto Puras (TST)	Added comments
v0.18	1 October 2021	Sonia Sotero (AYTOSAN)	Updated section 3.3 & 3.5
v0.19	1 October 2021	Mathieu Gallissot (CEA)	Included stress test report (section 2.4)
v0.20	4 October 2021	Keiko Doguchi (NTTE)	Updated section 3.5
v0.21	4 October 2021	Sonia Sotero (AYTOSAN)	Updated section 3.5

v0.22	5 October 2021	Orfeas Voutyras (ICCS)	Internal review
v0.23	5 October 2021	George Palaiokrassas (ICCS)	Updated section 3.6
V0.24	6 October 2021	Alberto Puras (TST)	Added Section 5 conclusions
V0.25	7 October 2021	Vanessa Clemente (WLI)	Answered to comments
V0.26	7 October 2021	Akira Tsuge (Keio)	Updated most internal review comments
V1.0	8 October 2021	Alberto Puras (TST)	Final Document

Table of Contents

Version history 3
Table of Contents 5
List of Tables 7
List of Figures 8
Glossary 9
1. Introduction 10
1.1 Scope of the document 10
1.2 Relation to other WPs and Tasks 10
2. Evaluation of the M-Sec tools & infrastructure 11
2.1 Requirements' fulfilment monitoring 11
2.2 Security Threats fulfilment monitoring 14
2.3 Components TRL and system's SRL 17
2.4 Description of the end-to-end tests 21
Test procedure 1 22
Test procedure 2 23
Test procedure 3 25
2.5 Key Performance Indicators 26
3. Qualitative and quantitative evaluation of the M-Sec Use Cases 40
3.1 General aspects 40
Qualitative evaluation 40
3.2 Pilot 1 (Use Case 1): Secured IoT devices to enrich strolls across smart city parks 41
Qualitative evaluation 41
Quantitative evaluation - Specific Key Performance Indicators 45
3.3 Pilot 2 (Use case 2): Home Monitoring Security System for ageing people 47
Qualitative evaluation 47
Quantitative evaluation - Specific Key Performance Indicators 50
3.4 Pilot 3 (Use case 3): Secure and Trustworthy Mobile Sensing Platform 53
Qualitative evaluation 53
Quantitative evaluation - Specific Key Performance Indicators 53

3.5 Pilot 4 (Use case 4): Secure Affective Participatory Sensing of City Events 58
Qualitative evaluation 58
Quantitative evaluation - Specific Key Performance Indicators 58
Cross-border 59
3.6 Pilot 5 (Use case 5): Smart City Data Marketplace with secure Multi-layer Technologies 70
Qualitative evaluation 70
Quantitative evaluation - Specific Key Performance Indicators 73
Cross-border 73
4. Cross-border replication 75
4.1 SmileCityReport new theme for city events 75
4.2 Marketplace for data, APIs and microservices 75
5. Conclusions 76

List of Tables

Table 1. Technology Readiness Level definitions. 17
Table 2. Asset's Technology Readiness Level table. 18
Table 3. System Readiness Level descriptions 19
Table 4. System Readiness Level of Use Case 1 19
Table 5. System Readiness Level of Use Case 2 20
Table 6. System Readiness Level of Use Case 3 20
Table 7. System Readiness Level of Use Case 4 21
Table 8. System Readiness Level of Use Case 5 21
Table 9. KPI for end-to-end security 22
Table 10. To design the future decentralized architecture of IoT 26
Table 11. Highly autonomous and secure interaction 29
Table 12. Security and trust in large scale autonomous and trust-less multipurpose smart city platform 30
Table 13. Future Decentralized IoT ecosystem 32
Table 14. UC1 Qualitative Evaluations Survey 42
Table 15. UC1 KPIs Results 45
Table 16. UC2 Qualitative Survey conducted to Atenzia 47
Table 17. UC2 Qualitative Survey conducted to end users 50
Table 18. UC2 KPIs Results 51
Table 19. UC3 KPIs Results 53
Table 20. UC4 KPIs Results 59
Table 21. UC4 Cross-border Qualitative Evaluations Survey in Santander 60
Table 22. UC4 Cross-border Qualitative Evaluations Survey in Fujisawa 65
Table 23. UC5 Crossborder Qualitative Evaluations Survey in EU and Japan 70
Table 24. UC5 KPIs Results 73

List of Figures

Figure 1: M-Sec Requirements Management methodology 11
Figure 2: Requirements fulfilment at the end of Y3. 12
Figure 3: M-Sec requirements distribution among levels of MoSCoW prioritization. 13
Figure 4: M-Sec requirements distribution among UCs and relevant stakeholders (absolute numbers). 13
Figure 5: Requirements distribution among different categories. 14
Figure 6: Progress towards covering the identified Security Threats. 15
Figure 7: Distribution of Security Threats based on the STRIDE categorization. 15
Figure 8: Distribution of Security Threats based on their type. 16
Figure 9: Distribution on Security Threats based on the layer they appear. 16
Figure 10: Distribution of Security Threats among UCs and stakeholders. 17
Figure 11. Topology used for the first test run 23
Figure 12. Stress test bench with 48 secured IoT gateways 23
Figure 13. Topology used for the second test run 24
Figure 14. Results of the benchmark 24
Figure 15. Third and final topology for the stress tests 25
Figure 16. Scalability test results 25
Figure 17: Screenshot of Twitter post (left) and external article (right) on the M-Sec e-consultation survey . 40
Figure 18: UC3 Pilot: Stage-1 Results 56
Figure 19: UC3 Pilot: Stage-2 Results 57
Figure 20: Screenshot from the Smile City Report 58
Figure 21: Cross border use of the Smile City Report 60

Glossary

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

1. Introduction

1.1 Scope of the document

Deliverable D2.8 “M-Sec validation and overall evaluation” is the outcome of Task 2.4 “Overall system validation and evaluation”, which focused on the evaluation of the M-Sec ecosystem through the feedback gathered from the M-Sec environment inhabitants and the technical validation of the M-Sec framework. To achieve these goals, testing activities and qualitative evaluations through several surveys were performed.

Regarding the surveys, the first one (the M-Sec e-consultation) covered the more general aspects, since it was aimed at collecting feedback from EU and Japanese citizens and stakeholders on their experience when using IoT devices and applications, as well as on their knowledge of EU and Japan’s data protection regulations. Other use case specific surveys were made to collect the direct feedback from the users of the different pilots.

In addition to the qualitative evaluation, within Task 2.4 the impact of the project was measured against a set of indicators.

This report is divided into the following sections:

- Section 2 Evaluation of the M-Sec tools and infrastructure, where a final update on the fulfilment of requirements, security threats management, TRLs, tests carried out, and Key Performance Indicators is provided
- Section 3 Qualitative and quantitative evaluation which describes the results obtained from the overall evaluation of the project, including the feedback gathered with the different surveys and evaluation of indicators per use case.
- Section 4 Cross border replication, where two additional ideas for cross-border replication are outlined.
- Section 5 Conclusions.

1.2 Relation to other WPs and Tasks

As already explained in the previous section this deliverable shows the results obtained within the Task 2.4 “Overall system validation and Evaluation”. This Task has as its main input the overall integration performed in Task 2.3, being the deliverable D2.7 “M-Sec integrated prototype – final release” one reference document for the execution of T2.4 and the preparation of this report.

In addition, this deliverable is closely related to T3.1 “System level and user level requirements” and T3.3 “Risks and security elements for a hyperconnected smart city”. In fact, the report provides the final update on requirements and security threats.

2. Evaluation of the M-Sec tools & infrastructure

2.1 Requirements' fulfilment monitoring

As presented in "D3.2 - M-Sec Requirements Analysis" during Y2, M-Sec devised and followed a **Requirements Management methodology** in order to complete Task 3.1 successfully and provide valuable results for other Tasks. Requirements Management consists of two phases: Requirements Elicitation and Requirements Analysis.

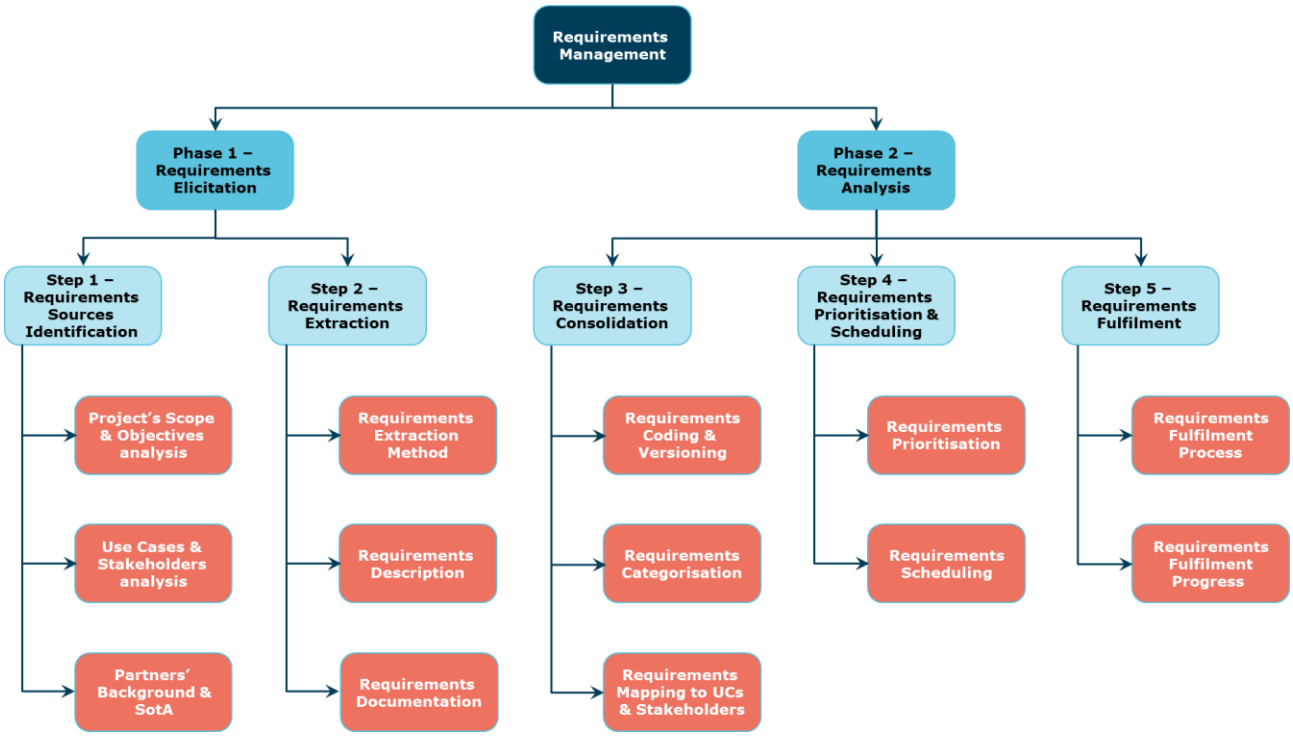


Figure 1: M-Sec Requirements Management methodology

The **Requirements Fulfilment** Step (5th column in the above figure) consists of all the processes required to identify how each requirement can be fulfilled and what the current level of fulfilment is. This step remained active during Y2 and Y3, to keep track of the fulfilment progress of each and every requirement.

The main tool used for the Requirements Management within the project was a spreadsheet, first included as Annex in D3.2. In the present deliverable, the last version of the spreadsheet is provided as an Annex (M-Sec_D3.2_Annex_v3.0).

Focusing on the evaluation perspective, for each requirement, the following fields are filled-in at the accompanying spreadsheet:

- Related to (Asset/FG): The asset (and FG) at which the requirement appears (if it does so).
- Covered by (Asset/FG): The asset (and FG) that can cover the specific requirement. This section is filled in by careful study of the available assets, as well as by mapping the Requirements Groups and Sub-

Groups to specific FGs and thus identifying potential assets that could be used. This process is described in D3.4.

- Covered through: The general approach followed to cover the requirement. If the requirement is covered by assets, then some specifications about this usage are presented. In some cases, no asset/FG group applies but a specific approach (e.g., best practices) has to be followed/ a specific decision has to be made.
- Undertaken by: The partner owning the asset that fulfils the solution or following up on the requirement's completion.
- Level of Fulfilment: The Progress values can be "0" for progress less than 33%, "1" for progress between 33% and 67%, "2" for progress between 67% and 99% and "3" for completed requirements. By using these values, a worst-case-scenario view is being provided. The level of fulfilment is related to the TRL, IRL and SRL of the assets, FGs and systems (as presented in Section 2.3).

As of Y2, for all requirements, an asset or approach covering them had been identified and the project presented a total progress towards requirements fulfilment of ~65%.

During Y3, out of the 139 requirements, 6 were identified as obsolete, and as such, their progress stopped being tracked ("NA" slice in the following figure). Moreover, two requirements of "Could" priority (following the MoSCoW system), were not 100% covered, as the corresponding functionalities to cover them were not implemented. However, the rest of 131 requirements were covered at a 100% level.

The above are shown in the following pie chart.

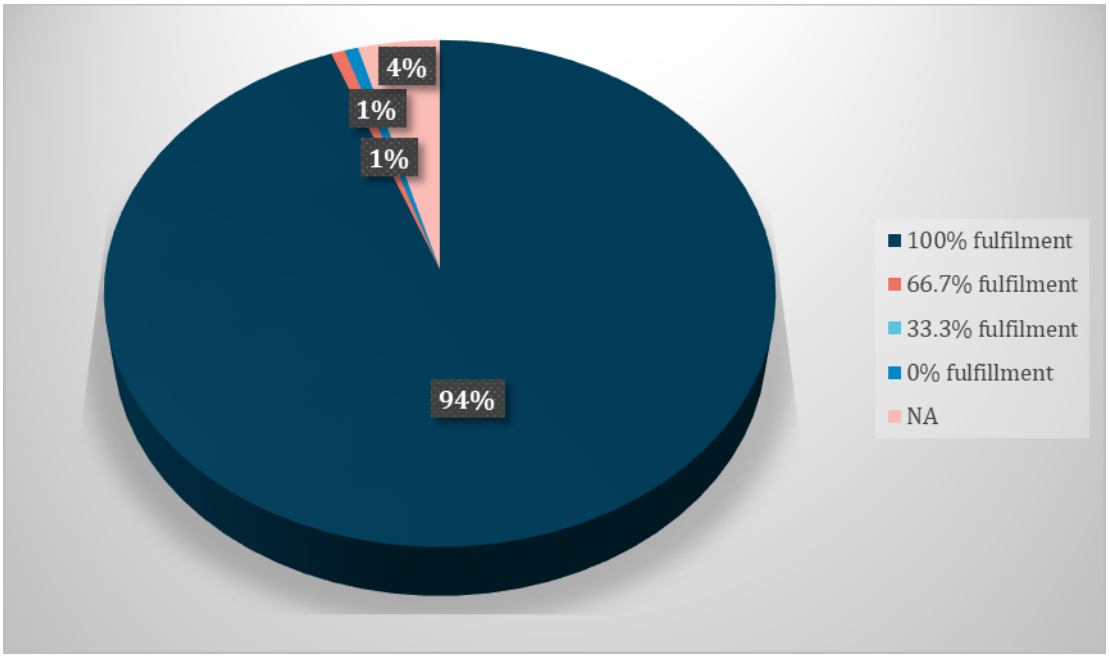


Figure 2: Requirements fulfilment at the end of Y3.

To sum up, 100% of all "Must" and "Should" requirements (not including the obsolete ones) have been completely fulfilled, with only two "Could" requirements in total not being completely covered.

The following figures give some overall statistics about the requirements.

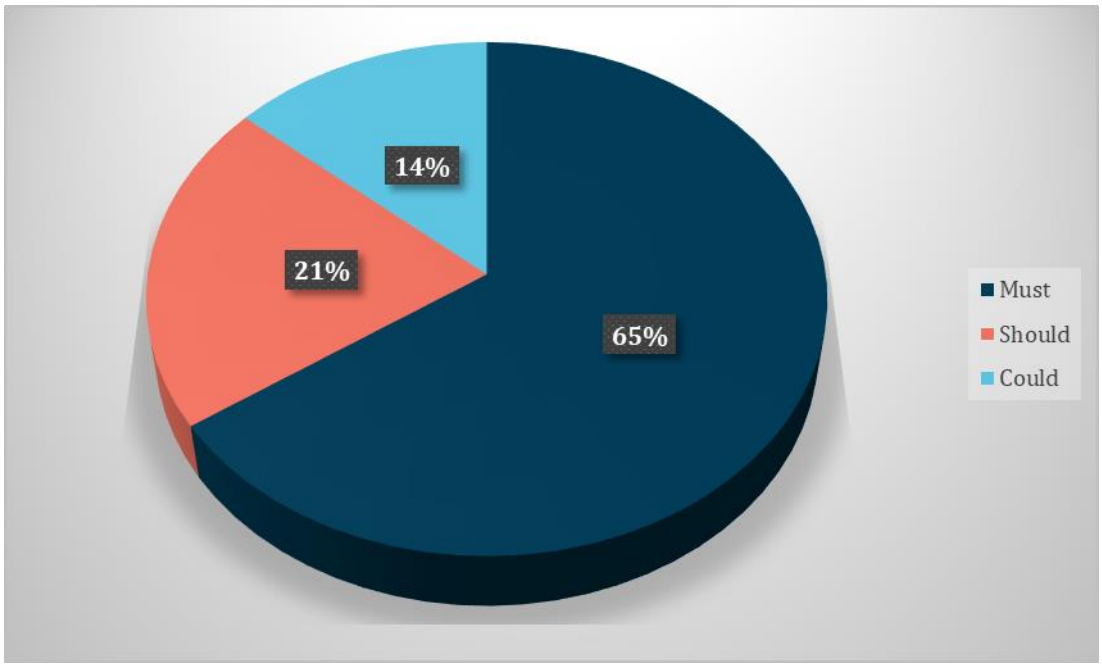


Figure 3: M-Sec requirements distribution among levels of MoSCoW prioritization.

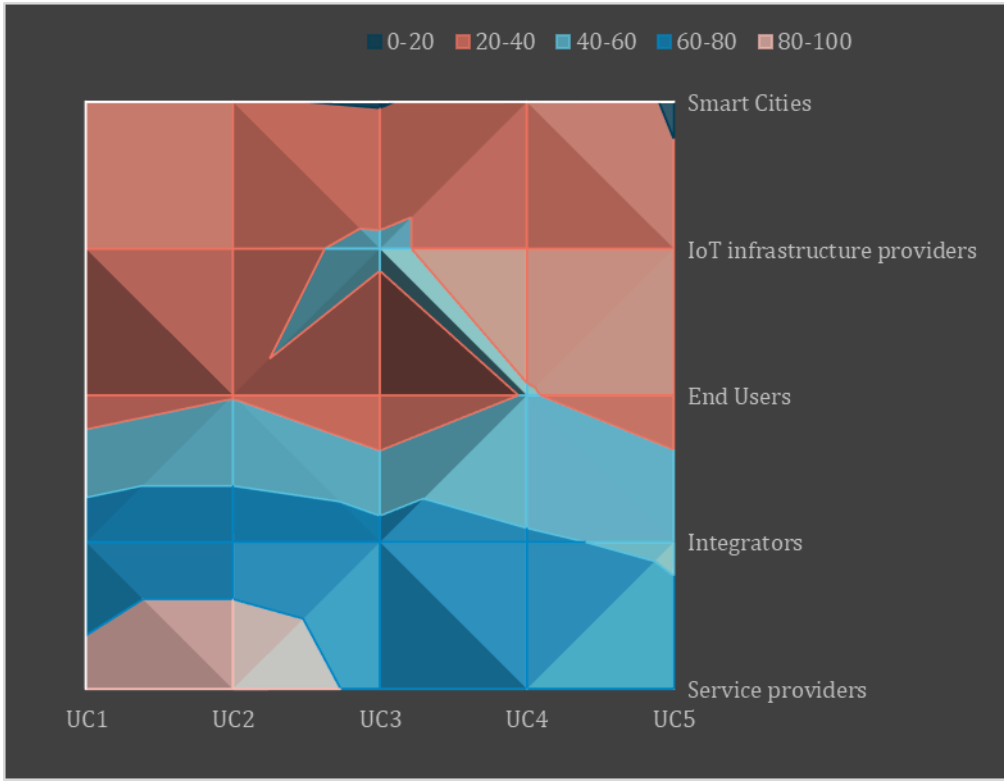


Figure 4: M-Sec requirements distribution among UCs and relevant stakeholders (absolute numbers).

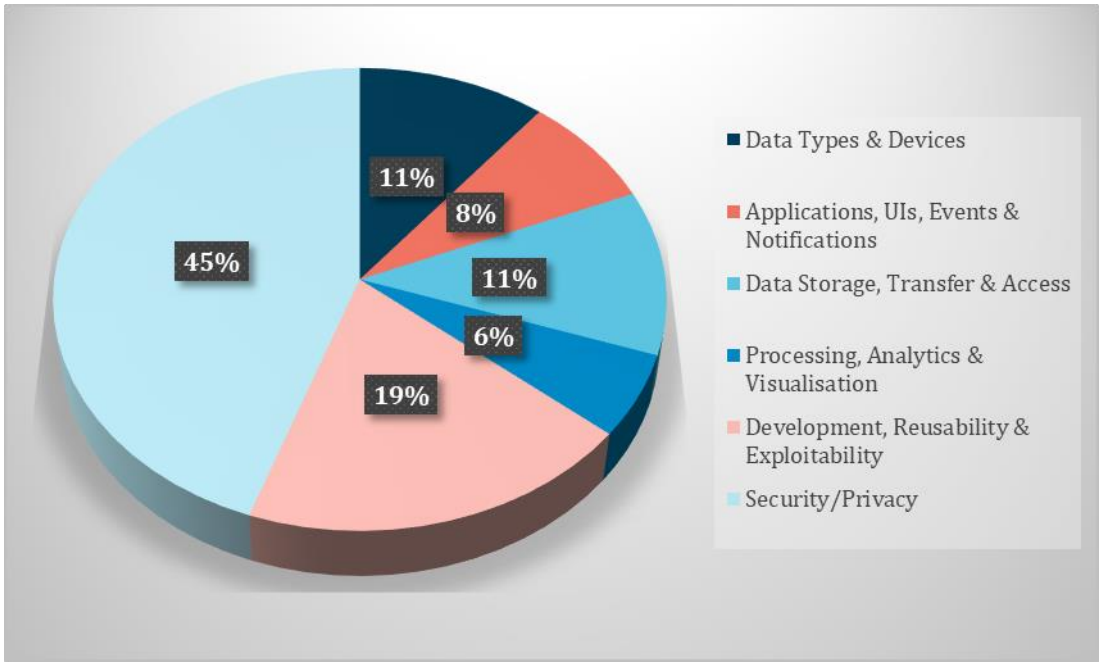


Figure 5: Requirements distribution among different categories.

2.2 Security Threats fulfilment monitoring

The overall security threats fulfilment was conducted as part of the **Security Threats Management cycle** to ensure that the identified threats have been mitigated properly. Overall, the methodology followed for the Security Threats Management was similar to the Requirements one (see Figure 1). Similarly, the main tool used for the Security Threats Management within the project was a spreadsheet, first included as Annex in D3.5. In the present deliverable, the last version of the spreadsheet is provided as an Annex (M-Sec_D3.5_Annex_v3.0).

During Y3, the mitigation assessment was also aligned with the NIST framework and helped in detecting any security weaknesses on an early stage. Periodic assessments ensured that the M-Sec assets were being monitored regularly and due diligence was taking place in order to protect assets from known and unknown threats. Timely patching of vulnerabilities can reduce the window of opportunity to exploit a vulnerable asset. A combination of technical controls, such as encryption, intrusion detection system, stealth security, patch management, and periodic threats assessments can help in addressing known and unknown threats.

Besides assessing the implementation of mitigating controls (as shown in the Annex), a new asset called "Stealth Security" was developed to make the devices invisible such that they do not reply to any unauthorized access, enquiries, or scans from the internet, except for authorized access. This feature has been introduced in the deliverable D4.2. In addition, a research paper has recently been published in the Journal of Information Processing Japan (September 2021)[1] on this topic.

[1] Bokhari, A.H., Inoue, Y., Kato, S., Yoshioka, K., and Matsumoto, T.: Empirical Analysis of Security and Power-Saving Features of Port Knocking Technique Applied to an IoT Device. Journal of Information Processing, Vol.29, pp.572-580 (2021). (DOI: 10.2197/ipsjjip.29.572)

All the details regarding the Security Threats mitigation and progress towards "covering" them are provided in M-Sec_D3.5_Annex_v3.0. Out of the 98 potential security threats identified in Y2 after running a security analysis on the M-Sec system, 26 of them were identified as non-applicable in Y3 ("NA" in Figure 6), either due to the non-existence of infrastructure on which the vulnerabilities can apply or due to some of the topics being out of the scope of the actual pilots.

The remaining 72 security threats that do apply to the final M-Sec system and pilots have been covered by 100%.

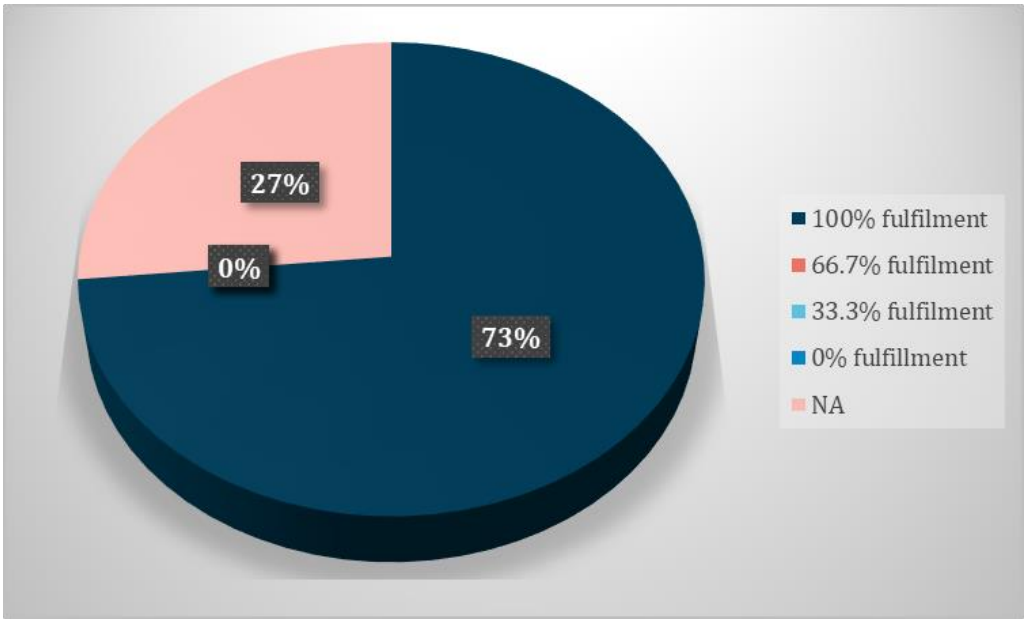


Figure 6: Progress towards covering the identified Security Threats.

The following figures provide some more statistics related to the security threats.

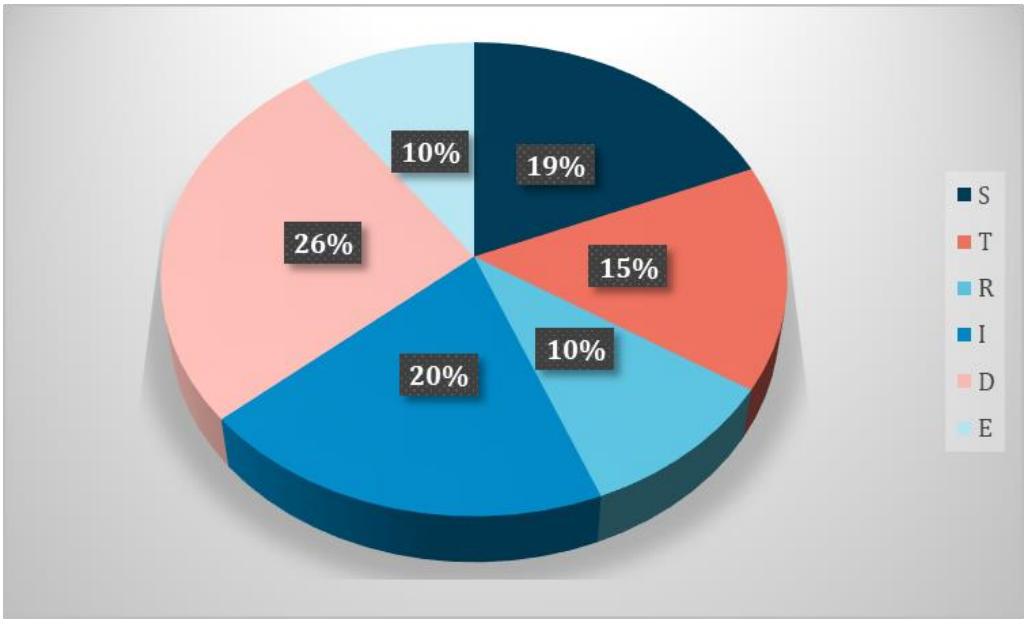


Figure 7: Distribution of Security Threats based on the STRIDE categorization.

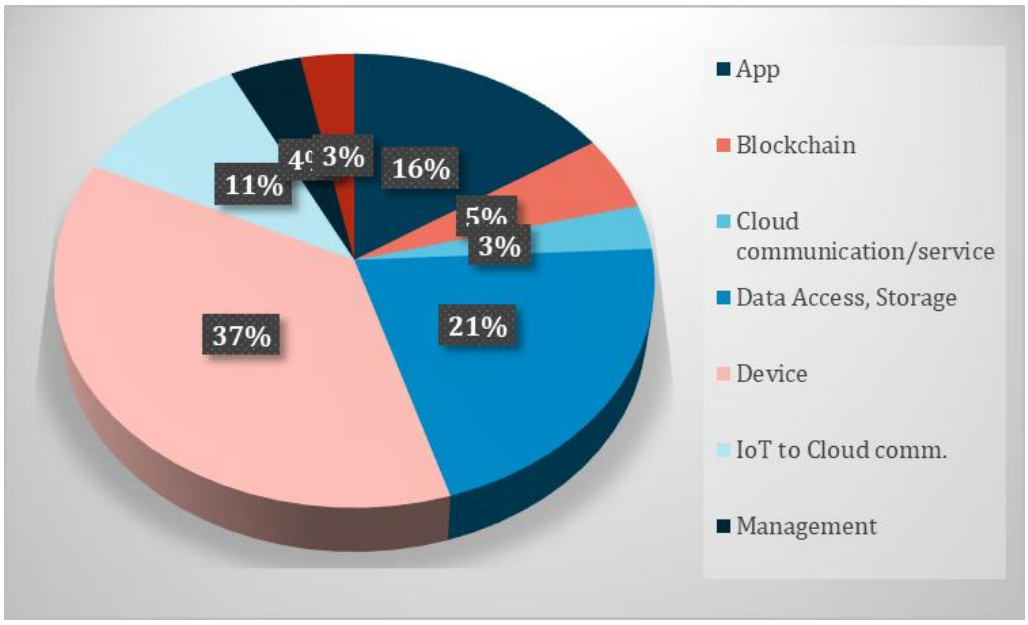


Figure 8: Distribution of Security Threats based on their type.

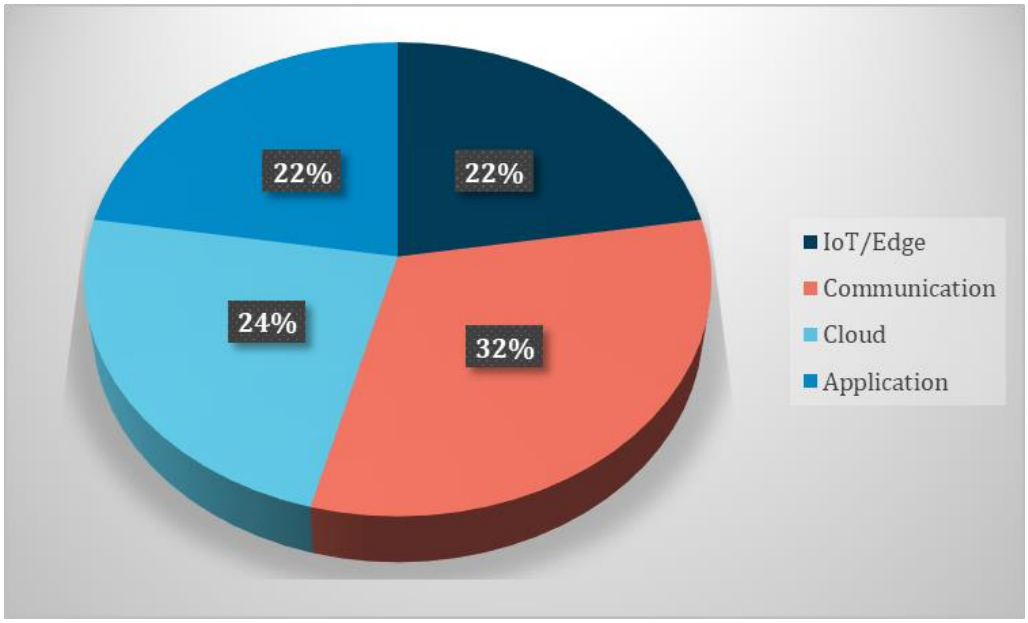


Figure 9: Distribution on Security Threats based on the layer they appear.

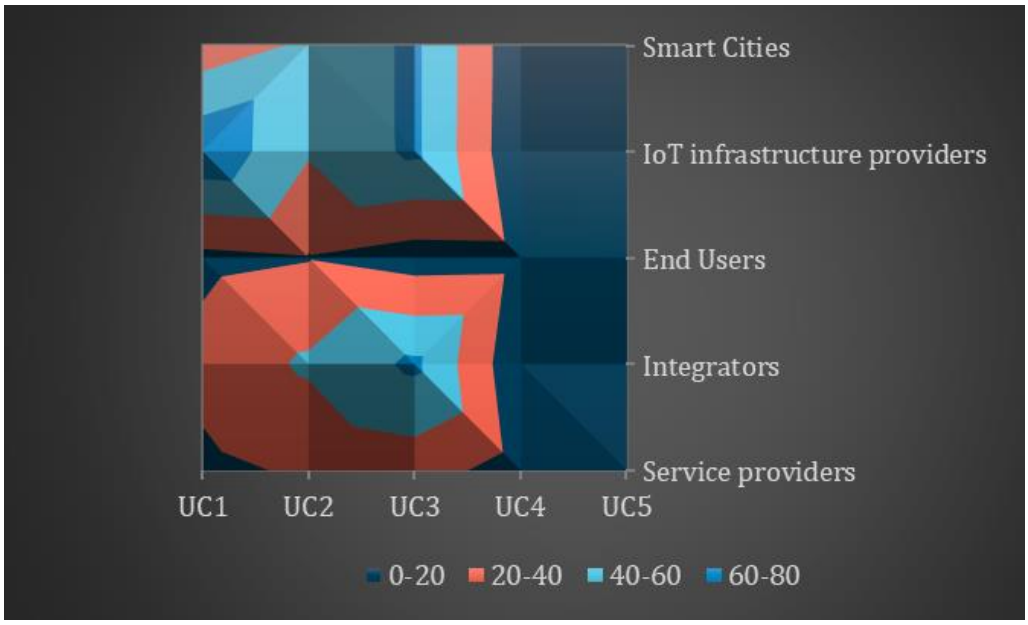


Figure 10: Distribution of Security Threats among UCs and stakeholders.

2.3 Components TRL and system's SRL

This section includes:

- A final list of the M-Sec components with the achieved TRL.
- The final number of the System Readiness Level per UC.

In Table 1 readers can find a reference with values and descriptions, to understand the Technology Readiness Level (TRL) scale.

Table 1. Technology Readiness Level definitions.

TRL	Definition/Description
9	Actual System Proven Through Successful Mission Operations
8	Actual System Completed and Qualified Through Test and Demonstration
7	System Prototype Demonstration in Relevant Environment
6	System/Subsystem Model or Prototype Demonstration in Relevant Environment
5	Component and/or Breadboard Validation in Relevant Environment
4	Component and/or Breadboard Validation in Laboratory Environment
3	Analytical and Experimental Critical Function and/or Characteristic Proof-of-Concept
2	Technology Concept and/or Application Formulated
1	Basic Principles Observed and Reported

Table 2 recaps the final TRL of all the components that are part of the final M-Sec prototype.

Table 2. Asset's Technology Readiness Level table.

FG	Component	Owner	TRL
Development and (Security) Designing Tools	Security Analysis Tool & Development Method for a Secure Service	NII	4
	Modal Transition System Analyzer	WU	7
Cloud Tools FG	Monitoring and Visualization Tool	YNU	6
Devices FG	Stealth Security	YNU	5
	Secured Component for Devices	CEA	6
	Intrusion Detection System	YNU	7
Privacy Management FG	Ganonymizer	KEIO	7
Secure City Data Access	Eclipse Sensinact Studio & Platform	CEA	7
	Secure SoxFire	KEIO	6
Secured & Trusted Storage FG	Quorum Blockchain /Blockchain Middleware	ICCS	7
	Crypto Companion Database	WLI	7
	T&R Model Engine/Tool	ICCS	6
IoT Marketplace FG	IoT MarketPlace	ICCS	9
End-to-End Security FG	Security Management Tool	CEA	5

Regarding the final number of the System Readiness Level per UC

In Table 3 readers can check a reference table, with value and description, to understand all values on System Readiness Level (SRL) as employed in this document. Additional information can be obtained in D2.7 Integrated prototype – final release.

Table 3. System Readiness Level descriptions.

SRL	Definition/Description
5	Operations & Support
4	Production & Development
3	System Development & Demonstration
2	Technology Development
1	Concept Refinement

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

Table 4 recaps the calculations performed to extract the Components SRL array for Use Case 1.

Table 4. System Readiness Level of Use Case 1.

Asset Name	TRL	Links	Non-normalized SRLi	Normalized SRLi	Component SRL
Park Guide	7	2	126	1,56	0,78
TST Server	7	4	224	2,77	0,69
IoT Marketplace	9	2	116	1,43	0,72
Eclipse sensiNact platform (and Studio)	7	6	290	3,58	0,60
Security Management Tool	5	3	143	1,77	0,59
TST IoT crowd-counting devices	7	4	203	2,51	0,63
TST IoT environmental devices	7	4	203	2,51	0,63
Secured components for devices and gateways	6	3	152	1,88	0,63
Quorum Blockchain framework	7	1	63	0,78	0,78
Honeypot (IoTPOT)	7	3	161	1,99	0,66
T&S FG API	7	4	196	2,42	0,60
Crypto Companion Database	7	2	112	1,38	0,69

After doing the calculations, the Composite SRL for Use Case 1 is 0.67, which is translated to an SRL of level 3 – System Development & Demonstration.

- Use Case 2 Home Monitoring Security System for Ageing People

Table 5 recaps the calculations performed to extract the Component SRL array for Use Case 2.

Table 5. System Readiness Level of Use Case 2.

Asset Name	TRL	Links	Non-normalized SRLi	Normalized SRLi	Component SRL
Worldline Connected Care Assistance	7	2	126	1,56	0,78
Worldline Server	7	5	287	3,54	0,71
IoT Marketplace	9	2	130	1,60	0,80
Eclipse sensiNact platform (and Studio)	7	4	196	2,42	0,60
Caburn Home Monitoring Devices	7	2	112	1,38	0,69
T&S FG API	7	5	245	3,02	0,60
Quorum Blockchain framework	7	3	161	1,99	0,66
Crypto Companion Database	7	3	161	1,99	0,66
Security Management Tool	5	3	143	1,77	0,59

After doing the calculations, the Composite SRL for Use Case 2 is 0.37, which is mapped to an SRL of level 3 – System Development & Demonstration.

- Use Case 3 Secure and Trustworthy Mobile Sensing Platform

Table 6 recaps the calculations performed to extract the Component SRL array for Use Case 3.

Table 6. System Readiness Level of Use Case 3.

Asset Name	TRL	Links	Non-normalized SRLi	Normalized SRLi	Component SRL
Secure SOXFire	6	5	250	3,09	0,62
Eclipse sensiNact platform (and Studio)	7	2	98	1,21	0,60
Node-RED	9	4	221	2,73	0,68
Modal Transition System Analyser (MTSA)	7	3	168	2,07	0,69
Security Management Tool	5	2	94	1,16	0,58
Visualization Tool	6	2	103	1,27	0,64
Deep Counter (Garbage Identification AI)	6	3	138	1,70	0,57
Secure Mobile Sensing Platform	6	5	212	2,62	0,52
Quorum Blockchain framework	7	1	63	0,78	0,78
Ganonymizer	7	3	168	2,07	0,69
Intrusion Detection System (IDS)	7	3	168	2,07	0,69
Honeypot (IoTPOT)	7	2	126	1,56	0,78
Stealth Security Component	5	2	75	0,93	0,46

After doing the calculations, the Composite SRL for Use Case 3 is 0.64, which is translated to an SRL of level 3 – System Development & Demonstration.

- Use Case 4 Secure Affective Participatory Sensing of City Events

Table 7 recaps the calculations performed to extract the Component SRL array for Use Case 4.

Table 7. System Readiness Level of Use Case 4.

Asset Name	TRL	Links	Non-normalized SRLi	Normalized SRLi	Component SRL
SmileCityReport (App)	8	5	280	3,46	0,69
SmileCityReport (Server)	8	4	231	2,85	0,71
Ganonymizer	7	2	119	1,47	0,73
Secure SOXFire	6	4	211	2,60	0,65
Security Management Tool	5	1	45	0,56	0,56
IoT Marketplace	9	4	191	2,36	0,59
Security Analysis tool + Development Method for secure Services	4	1	36	0,44	0,44

After doing the calculations, the Composite SRL for Use Case 4 is 0.63, which is translated to an SRL of level 3 – System Development & Demonstration.

- Use Case 5 Smart City Data Marketplace with Secure Multi-Layer Technologies.

Table 8 recaps the calculations performed to extract the Component SRL array for Use Case 5.

Table 8. System Readiness Level of Use Case 5.

Asset Name	TRL	Links	Non-normalized SRLi	Normalized SRLi	Component SRL
Iot Marketplace	9	11	440	5,43	0,49
Worldline Server	7	2	126	1,56	0,78
Secure SOXFire	6	2	99	1,22	0,61
SmileCityReport (App)	8	2	117	1,44	0,72
SmileCityReport (Server)	8	2	117	1,44	0,72
T&R Model engine/tool	6	3	130	1,60	0,53
Node-RED	9	3	225	2,78	0,93
Quorum Blockchain framework	7	7	301	3,72	0,53
Mobile Wallet	7	3	79	0,98	0,33
Eclipse sensiNact platform (and Studio)	7	4	183	2,26	0,56
Security Management Tool	5	4	133	1,64	0,41

After doing the calculations, the Composite SRL for Use Case 5 is 0.60, which is translated to an SRL of level 3 – System Development & Demonstration.

2.4 Description of the end-to-end tests

In this section, we include the description and the obtained results from the stress tests conducted to validate the performance of the technical components and to verify the objectives of the project, especially the KPIs that are listed in Table 9. These KPIs aim to illustrate the performance of the technical architecture proposed in the project, in particular the performance of the security layer.

Table 9. KPI for end-to-end security

KPI	Minimum Target	Achieved
Number of end-to-end secure communication data stream accommodated by M-Sec	100,000	Up to 500,000
Response time	<1sec	Few milliseconds for a regular usage

The verification of these KPIs was made within a scalability test by CEA with support from other technical partners. The goal of this scalability bench was to push an M-Sec representative topology to its limits. Regarding the end-to-end communication, we proposed a comparison between an unsecured communication and a secure one to quantify the overheads brought by the security layer.

Context of tests:

- End-to-end secure communication data stream is a message sent from an IoT device to an endpoint hosted in the cloud. This message is secured by 1) a TLS asymmetric encryption based on certificates provisioned by the M-Sec security manager and 2) authentication of the source based on a signature managed by the M-Sec security manager to verify the authenticity of the sender. The number of streams corresponds to the number of simultaneous data sources that can send messages to the endpoint. Using the MQTT protocol, it corresponds to the number of publishers that can be handled by the subscriber without collapsing.
- Response time corresponds to the latency of the infrastructure. It is measured using acknowledge messages, so it corresponds to a round-trip latency of secured messages. It is expected to have better performance in non-acknowledged

Limits of the tests

The topology under test was simulated with limitations regards real infrastructure, especially in simulation of external factors such as network latency, QoS, bandwidth, availability, etc. Those factors are external to the M-Sec security layer which is under test but may impact the KPI out of a laboratory environment.

Regarding the first KPI, we made a test with up to 500,000 publishers without noticing collapse even though the response time was degraded. Regarding scalability, a solution such as load-balancing mechanism can be used.

Test procedure 1

Initially, to conduct the test, CEA has built a reference platform with 48 IoT devices and a server. This bench is illustrated in Figure 12 and the architecture in Figure 11. These devices use a similar design with the one used in UC1. They are enrolled in the security manager with unique certificates which can be used for the application layer. The application layer is made of a script, that sends data in controlled infinite loops using

the MQTT protocol in an encrypted and authenticated way, using the previously provisioned certificates. The performance can be modified by tuning the multi-threading part and the sleeping time of the script's loop.

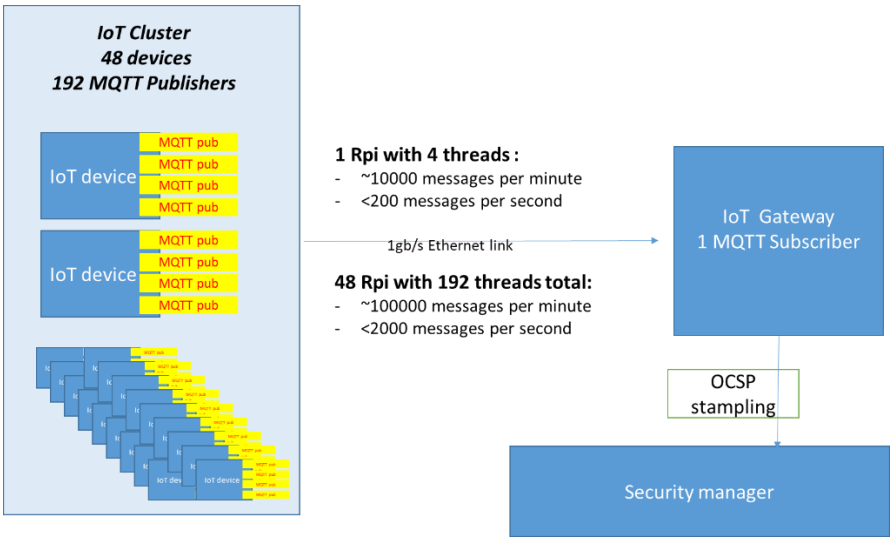


Figure 11. Topology used for the first test run

Thus, the performance was poor due to high network contention and low computing resources from the IoT devices, which we used in an intensive manner.

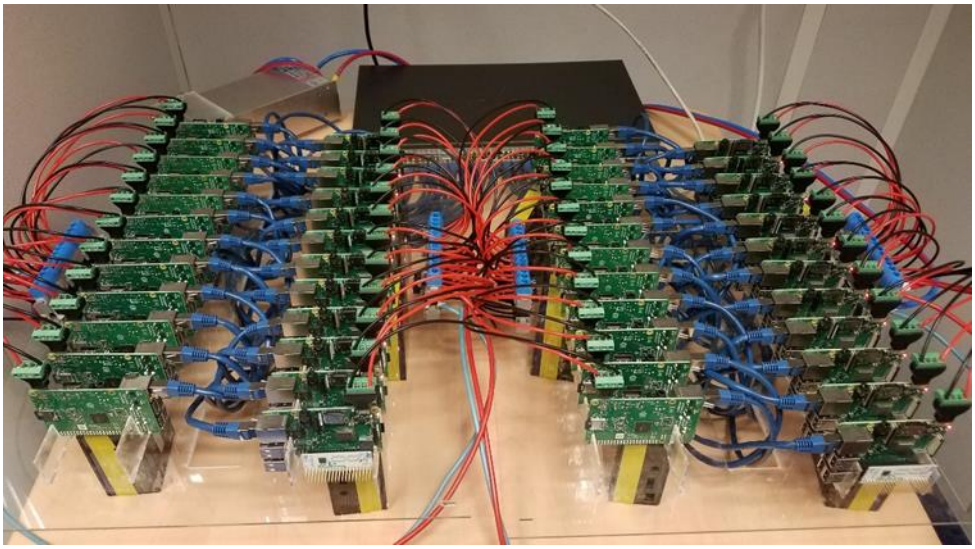


Figure 12. Stress test bench with 48 secured IoT gateways

Test procedure 2

To overcome the difficulties found in the first bench, we have leveraged virtualization to reduce the impact of poor network design or poor device performance. At first, we introduced a load balancer and multiple instances of MQTT brokers to manage the server's side performance. Then, we virtualized a client with many threads on the same host as the server to mitigate network contention and to increase the publisher's global performance. Figure 13 shows the updated topology.

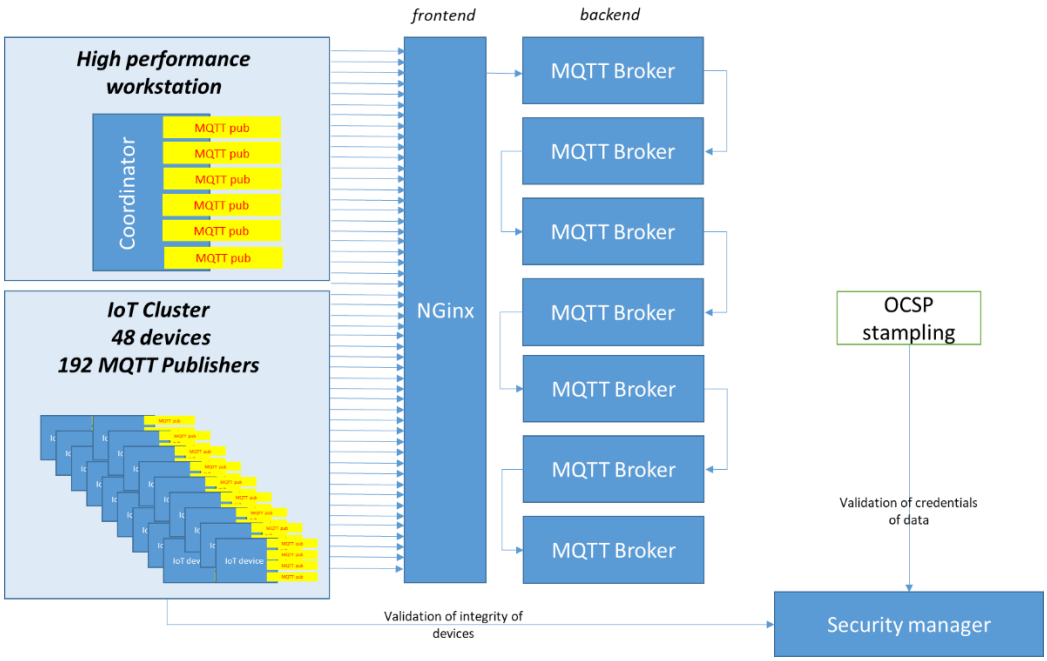


Figure 13. Topology used for the second test run

Also, in order to calibrate the load balancing, we have run the client iteratively, by increasing the amount of data sent in a progressive manner. Figure 14 shows the results of this benchmark with the y axis indicating the response time +10s (arbitrary delay) and the x axis the messages per second which were sent.

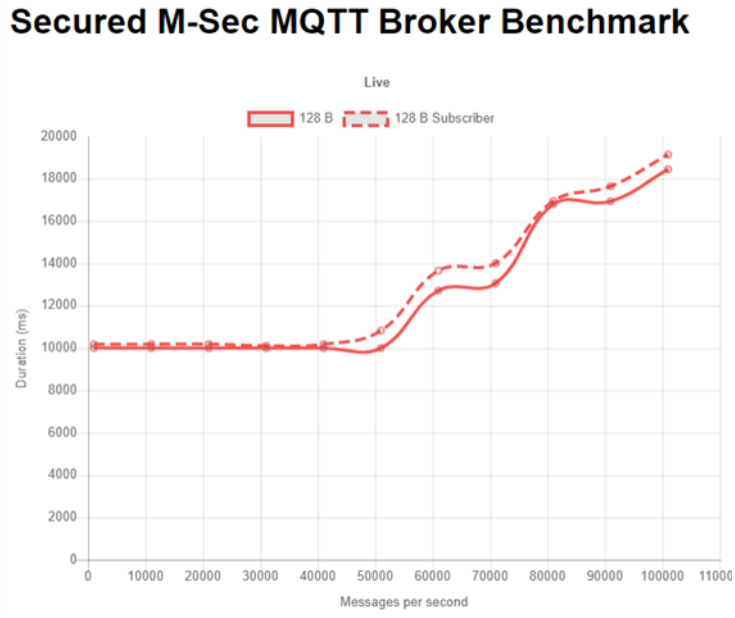


Figure 14. Results of the benchmark

Test procedure 3

To focus on optimization and performance, we ran a 3rd test based on recommendations proposed in https://stackoverflow.com/a/36377681 and https://github.com/hui6075/mosquitto-cluster.

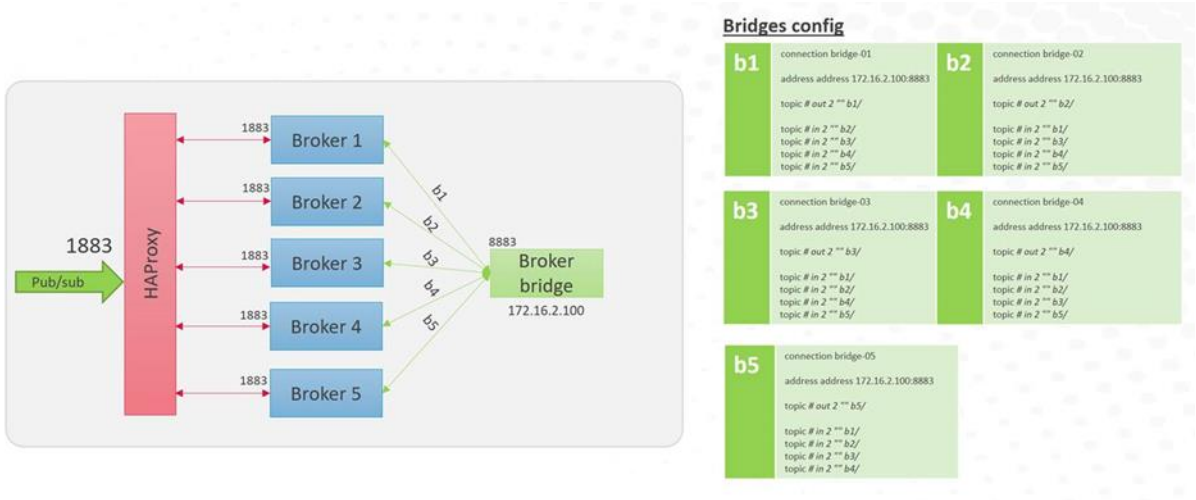


Figure 15. Third and final topology for the stress tests

The test was executed 5 times to have an average, results are in

Figure 16. In red, the topology with 10 brokers and in purple with 5 brokers. We can see that there is an impact on the number of brokers only in unsecure mode (dotted lines) but not in the secure mode. The response time is very good until we reach about 40.000 messages per second in which queues and delays start to have an impact in a linear way. But still around 1.5s for 100.000 messages per second.

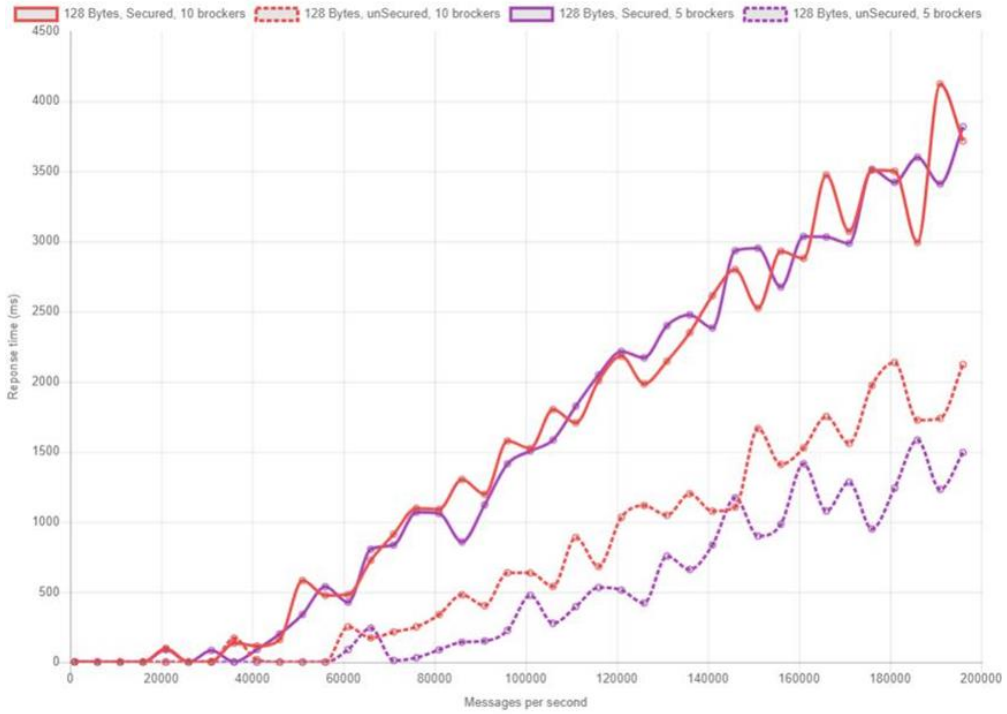


Figure 16. Scalability test results

2.5 Key Performance Indicators

In this section an overview of the KPIs used for the development of the M-Sec infrastructure is provided.

Table 10. To design the future decentralized architecture of IoT

Objective 1: Decentralized architecture of IoT				
Sub-objectives	**Key Indicators**	**Minimum target**	**Achieved**	**Description**
1.1 Architecting approaches to develop different delivery and communication patterns	Number of supported communication patterns	3	3	The consortium has identified three communication patterns: • P2P (Quorum Blockchain framework) • Client/server (SensiNact Secure IoT Middleware) • Publish/subscribe (End-to-end Encryption Middleware for SOXFire)
	Number of supported concepts/ contexts	3	4	In terms of number of support contexts based on proximity or location, availability, common goals and interests, the consortium has identified: • Public IoT data (temperature, noise, humidity, etc.) from the mobile sensing scenario (UC3) and environmental sensors (deployed on UC1 and visualized with The Park Guide Application). • Photos Images and metadata from the UC4 • Smart Home Monitoring Data from UC2 • Trust & Reputation related data
1.2 Performing a thorough Risk Assessment Study	Number of risk assessment cycles conducted	1	1	During the second year of the project, a risk assessment was conducted within D3.5 and threats were categorized into IoT devices, gateways, cloud, and application following the STRIDE Model, a useful tool to

Objective 1: Decentralized architecture of IoT				
Sub-objectives	**Key Indicators**	**Minimum target**	**Achieved**	**Description**
				help classify threats. STRIDE stands for Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privilege. In addition, during third year, threats and risks file has been updated with new ones and it can be found within this deliverable D2.8 M-Sec validation and overall evaluation.
	Number of risks identified	10	72	As part of the T3.3 execution, 98 threats were considered. 26 of them are non-applicable to M-Sec framework, while 72 have been mitigated (100% fulfilment).
1.3 Introducing mechanisms to establish seamless hyper-connectivity over heterogeneous communication channels	Number of supported communication channels	5	5	Five supported communication channels have been identified: • UC1: Low-Power Wide-Area Network (NB-IoT) • UC2: Short-range radio technology (Zigbee protocol) • UC3: Long-Term Evolution (LTE) • UC4: Mobile Communication-GSM • UC1-5: Permissioned blockchain
1.4 Introducing a virtualization layer between the abstracted and actual resources	Number of device adaptors provided	100	252	From the different UCs that validate the M-Sec framework, we have identified the following number of device adaptors by UC: • UC1 Adaptors: 7 Types of measurements provided by 6 devices: temperature, humidity, CO_2, VOC, noise,

Objective 1: Decentralized architecture of IoT				
Sub-objectives	**Key Indicators**	**Minimum target**	**Achieved**	**Description**
				MAC Wi-Fi counter, MAC BT counter ○ 5 EnMon devices * 5 sensors = 25 adaptors ○ 1 Crow devices * 2 sensors = 2 adaptors • UC2 Adaptors: 10 types of measurements provided by 5 devices: Motion (presence, temperature, light) door/window (open or closed + temperature), smart plug (power, current, voltage, ac frequency), occupancy sensor (weight). In total: 50 adaptors. • UC3 Adaptors: ○ Garbage Trucks' sensing: 9 types of measurements provided by 15 devices: Acceleration, Angular Velocity, Geomagnetism, Atmospheric Pressure, UV-A, Illumination, Temperature, Humidity, PM2.5. In total: 135 adaptors. ○ Restaurant environment sensing: 4 types of measurements provided by 10 devices: CO2, PM2.5, Temperature, Humidity. In total: 40 adaptors.
	Number of actual resources	1,000	2,848	• Secure SOXFire provides access to 2,829 sensor resources • 8 sensor node resources are operated on top of the secure KEIO Mobile Sensing Platform to realize UC3

Objective 1: Decentralized architecture of IoT				
Sub-objectives	**Key Indicators**	**Minimum target**	**Achieved**	**Description**
				• 6 sensor device resources are operated on top of M-Sec platform to realize UC1 • 5 sensor device resources are operated on top of M-Sec platform to realize UC2

Table 11. Highly autonomous and secure interaction

Objective 2: Highly autonomous and secure interaction				
Sub-objectives	**Key Indicators**	**Minimum target**	**Achieved**	**Description**
2.1 Designing and implementing a constrained multi-objective optimization approach	Number of objectives to be optimized: e.g. availability, importance, functional relevance according to the overall purpose of desired interaction pattern	>5	6	• Trust and Reputation Module capable of measuring: o Reliability o Reputation o Trustworthiness, o Availability. • Privacy settings are also considered and are an integral point of all decision-making procedures. • Communication tool between Sensinact & SoxFire (to choose one or the other one).
2.2 Enabling adaptation of service chains following their repurposing requirements	Time needed to perform the adaptation in the flow of service chain	<1 sec	<1 sec	Permissions in the blockchain/Marketplace ecosystem can be changed under the desired time limit. In addition, the implementation of new Smart Contracts is also executed under this specific time limit.
	Security requirements considered for this	>4	>5	Permissions of data/services providers are restrained based

Objective 2: Highly autonomous and secure interaction				
Sub-objectives	Key Indicators	Minimum target	Achieved	Description
	adaptation: e.g. threat possibility, confidentiality level, access rights, authentication mechanism			on trust, reputation and reliability. Also, permissions of consumers are also restrained based on the level of Privacy (see confidentiality, authentication, and access levels) that the provider wants to achieve. Mechanisms to handle DDoS attacks are also in place.

Table 12. Security and trust in large scale autonomous and trust-less multipurpose smart city platform

Obj3. Security and trust in large scale autonomous and trust-less multipurpose smart city platforms				
Sub-objectives	Key Indicators	Minimum target	Achieved	Description
3.1 Defining and implementing a lightweight blockchain public ledger and the trust ensuring mechanisms	Number of blockchain implementations piloted for the purposes of use cases	>2	2	• Quorum Network • Ethereum Network
	Number of peer nodes sustaining the blockchain during the operation of the pilots	>6 nodes	>126	Alastria in total hosts 126 nodes (https://alastria.io/socios-nodos/)
3.2 Developing mechanisms that can facilitate end-to-end security across the whole path from IoT sensor to edge and cloud computing	Number of end-to-end secure communication data stream accommodated by M-Sec	100,000	Up to 500.000	Tests conducted with up to 500,000 publishers without noticing collapse even thou the response time was degraded.
	Response time	<1 sec	Few msec for a regular usage	
3.3 Defining and implementing automatic verification	Overall latency overhead for automatic verification	<1 sec	<500 msec	Automatic verification and self-repair mechanism for work-flow-based smart city applications, adopt model-

Obj3. Security and trust in large scale autonomous and trust-less multipurpose smart city platforms				
Sub-objectives	**Key Indicators**	**Minimum target**	**Achieved**	**Description**
and self-repair mechanisms	and self-repair mechanisms			based verification and self-adaptation mechanism with controller synthesis tool called MTSA. We have already tested with small smart city application example in laboratory, and ensured that the synthesis and translation into Node-RED model can finish within 500 msec.
3.4 Engineering a Multi-Layer Security and Privacy Analysis framework	Number of successful analysis experiments	9 (3 per use case)	Each use case with over 4 Successful analysis experiments	Task 3.2 M-Sec Architecture and T2.3 Overall integrations, identifies the functional groups as well as the assets which integrated them and that are used per use case. Based on that, the number of successful analysis experiments conducted per UC are as follow: • UC1: 5 analysis experiments • UC2: 4 analysis experiments • UC3: 8 analysis experiments • UC4: 5 analysis experiments • UC5: 4 analysis experiment

Table 13. Future Decentralized IoT ecosystem

Obj4. Future decentralized IoT ecosystem				
Sub-objectives	Key Indicators	Minimum target	Achieved	Description
4.1 Developing a novel marketplace	Smart objects joining the marketplace	1,000	2,829	

Obj4. Future decentralized IoT ecosystem				
Sub-objectives	Key Indicators	Minimum target	Achieved	Description
ewhere	tplace			
smart objects can exchange in	Total exchange of virtual cu	10,000 unit	40,860 M-Sec Tokens	

Obj4. Future decentralized IoT ecosystem				
Sub-objectives	Key Indicators	Minimum target	Achieved	Description
formation, energy and services thro	rrencies for virtual goods trade via			

Obj4. Future decentralized IoT ecosystem				
Sub-objectives	Key Indicators	Minimum target	Achieved	Description
ughthe useof virtualcurrencies	themarketplace			
4.	Nu	4 (	4 pilots level	

Obj4. Future decentralized IoT ecosystem				
Sub-objectives	Key Indicators	Minimum target	Achieved	Description
2 Creating demonstrators and ecosystems	number of demonstrators	2 per city)	demonstrators (2 per city) + 1 “global” one > 4 FGs and subsystems demonstrators	
	Number of use	2	2 per subsystem and 4 per subsystem/ FG	

Obj4. Future decentralized IoT ecosystem				
Sub-objectives	Key Indicators	Minimum target	Achieved	Description
tems for real-life use cases	case per demonstrator			
Develo	Applic	5	9	9 Teams presented their ideas on the Online Contest conducted during the week of 6th to 10th September 2021. Six of them (three per each city challenge, were awarded)

Obj4. Future decentralized IoT ecosystem				
Sub-objectives	Key Indicators	Minimum target	Achieved	Description
ping innovative ideas through the in	ations built with new ideas during th			

Obj4. Future decentralized IoT ecosystem				
Sub-objectives	Key Indicators	Minimum target	Achieved	Description
volvement of new entrants	eprojectlifetime			

3. Qualitative and quantitative evaluation of the M-Sec Use Cases

3.1 General aspects

Qualitative evaluation

The M-Sec e-consultation survey was launched on December 2020 and ran until September 2021 to all EU and Japanese citizens and stakeholders, considered as potential users of the M-Sec framework, to collect feedback on their experience when using IoT devices and applications and on their knowledge of EU and Japan's data protection regulations. The main goal of this survey was to help the project better understand the IoT ecosystem in which M-Sec was expected to operate, what were people's main IoT habits and their awareness regarding data protection regulation in their regions.

The survey was launched in English and then later translated to Spanish and Japanese, for a larger outreach. At the end of the project, the consortium was able to collect 355 answers in English, 206 in Japanese and 33 in Spanish, a total of 594 answers. The e-consultation survey was widely disseminated through M-Sec's main communication channels – dedicated blogpost, social media posts, newsletters, call for action by email invitation, etc. – and a social media campaign was launched between March and April 2021 on LinkedIn and Twitter to promote the survey and engage new stakeholders. M-Sec has also disseminated the survey in other online communities and media, such as Cyberwatching.eu and StandICT.eu H2020 networks, among others, apart from its internal network of contacts.

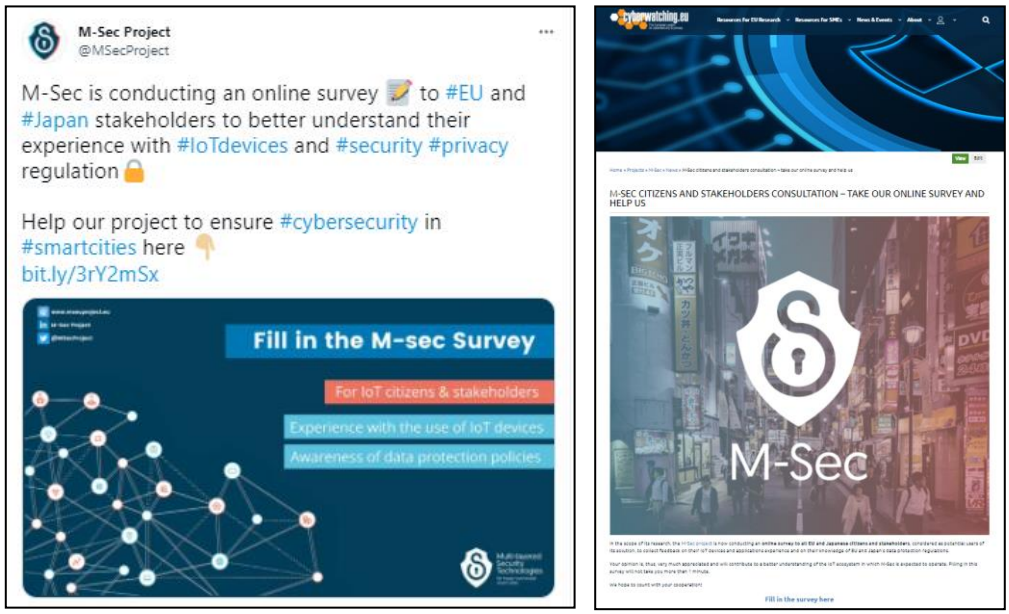


Figure 17: Screenshot of Twitter post (left) and external article (right) on the M-Sec e-consultation survey

After 6 months, with a sample of 450 answers, the consortium decided to do a preliminary analysis of the answers to the survey. These results were then made public to the M-Sec community through a dedicated blogpost. The main results were as follows:

- **IoT habits. Will devices and apps become part of citizen's daily routines?** Most respondents (22%) identified health devices – such as fitness bracelets – as the IoT device that they most commonly use, closely followed by home appliances (21%) – such as smart refrigerators – and voice assistants (21%) – such as Google Home or Alexa. 34% of respondents seem to use those devices every day, all day, which shows they are increasingly becoming part of citizens daily lives and routines.
- **IoT security and privacy concerns. Are citizens aware of such dangers when using IoT devices?** As the use of IoT devices and apps becomes increasingly higher in today's modern and connected society, security and privacy concerns related with their use must be taken into consideration by all, as we exchange more data than before – data that, sometimes, might be sensitive and personal. However, 64% of our respondents are not fully aware of security and privacy data protection policies of the IoT devices and apps they so commonly use, meaning that they do not always carefully read those policies when start using a device or app or when those policies are updated by the provider. Thus, it becomes extremely important to raise awareness among citizens and stakeholders regarding the dangers of such use, the attacks they might suffer, and the loses they might have, and how we, individually and as a society, can fight it or, better yet, prevent it from even happening. In fact, when confronted with a hypothetical scenario in which a given IoT device or app suffers a cyber-attack, most respondents (52%) prefer to stop using that device or app immediately and then go and check its data protection policies. Therefore, the M-Sec Project has created a Comic Book – English and Japanese version – that we hope will help citizens better understand what is at stake when it comes to the security and privacy of their data and how the M-Sec solution will help them prevent several types of cyber-attacks when they are using a given IoT device or app, which they believe might facilitate their lives. In fact, the main privacy and security concerns seem to be more related wrongful use of data by others (>60%), than the actual malfunction of the IoT device or app itself.
- **IoT policy. Are citizens aware of data protection policies?** Although most respondents (89%) do not seem to be aware of the current IoT smart city solution deployed in their city, they are aware of small changes at a city or even at a more local level (for instance, in neighbourhoods), that clearly positively affect their lives. Some examples are C02 and air quality sensors, transportation, parking and traffic related sensors, smart gardening and watering related sensors, smart building automation for public buildings, open data portals, among other small-scale initiatives. Moreover, when asked about EU and Japan's GDPR and APPI's data protection regulations, EU and Japanese respondents show a satisfactory level of awareness – either they are fully aware or, at least, have heard about it.

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

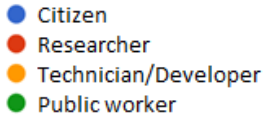
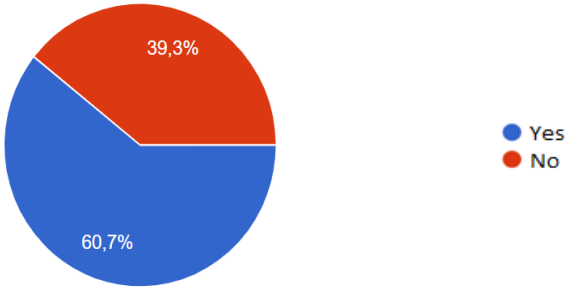
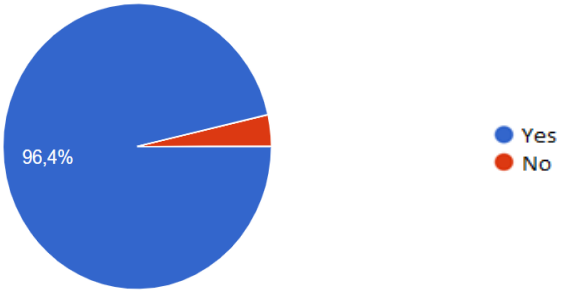
Qualitative evaluation

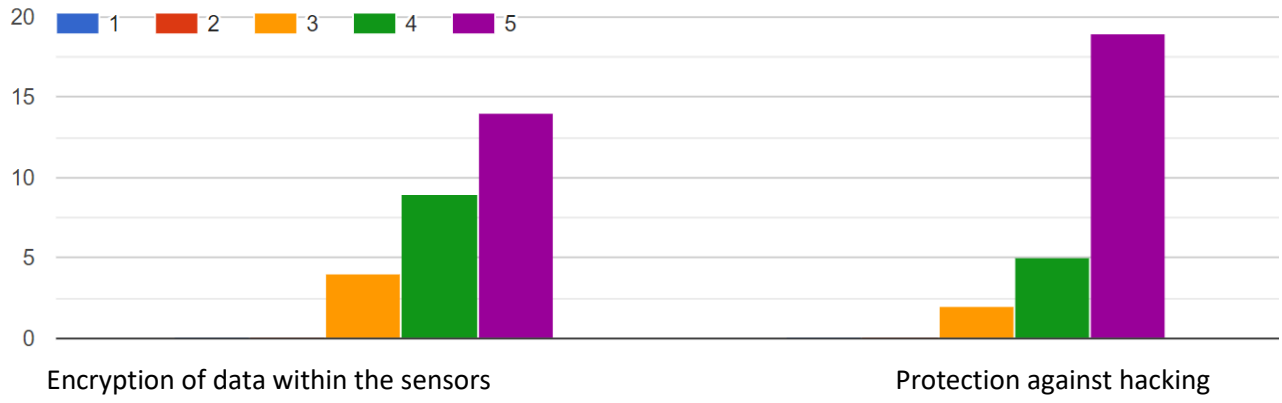
The qualitative evaluation was addressed through a user survey to try to get more in-depth feedback. The survey was elaborated in such a way that all the most important aspects of the pilot are covered. In this regard,

questions about security, privacy, as well as the implementation of the pilot were included. Besides, the language was adapted to avoid too complex questions that might lead to unusable responses.

The survey was implemented with the Google Forms service, a web application that allows the fast and easy creation of surveys. The link to the survey was included in the Park Guide application to give users the possibility to provide their feedback. The following table shows the questions and users' answers.

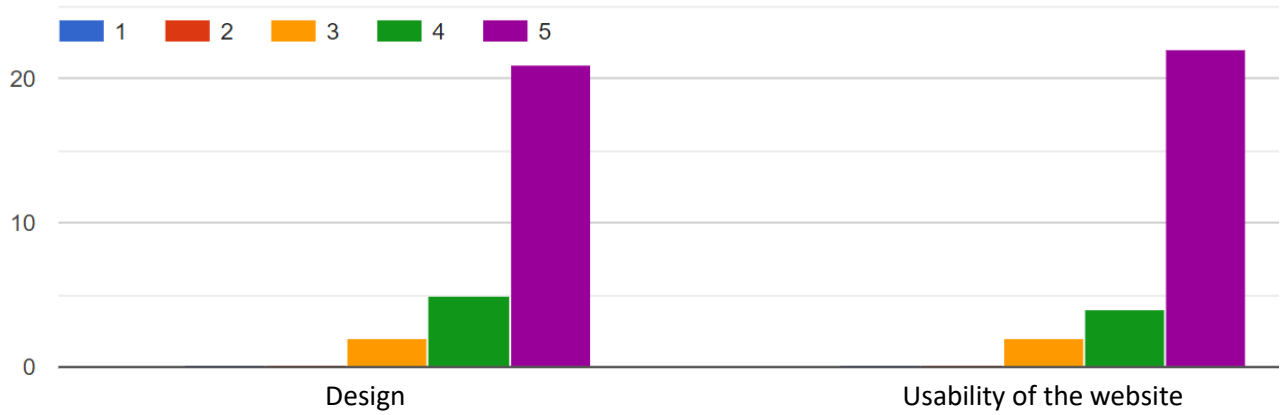
Table 14. UC1 Qualitative Evaluations Survey

User profile

Previous experience with sensors and Smart Cities

Awareness of privacy issues related to the use of your personal data in this pilot

Importance of the following functionalities **(1 = No important – 5 very important)**



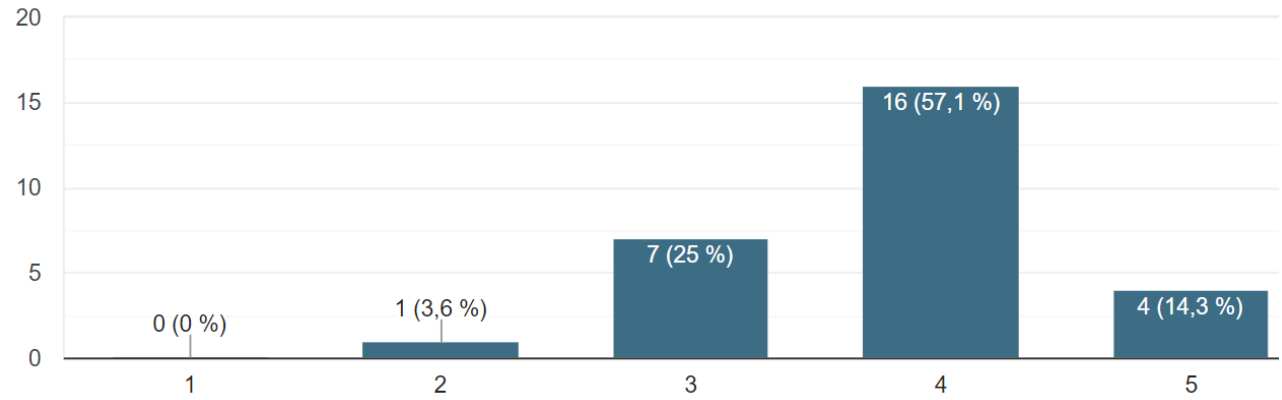
Regarding the website

(1 = Do not like it – 5 = I like it very much)



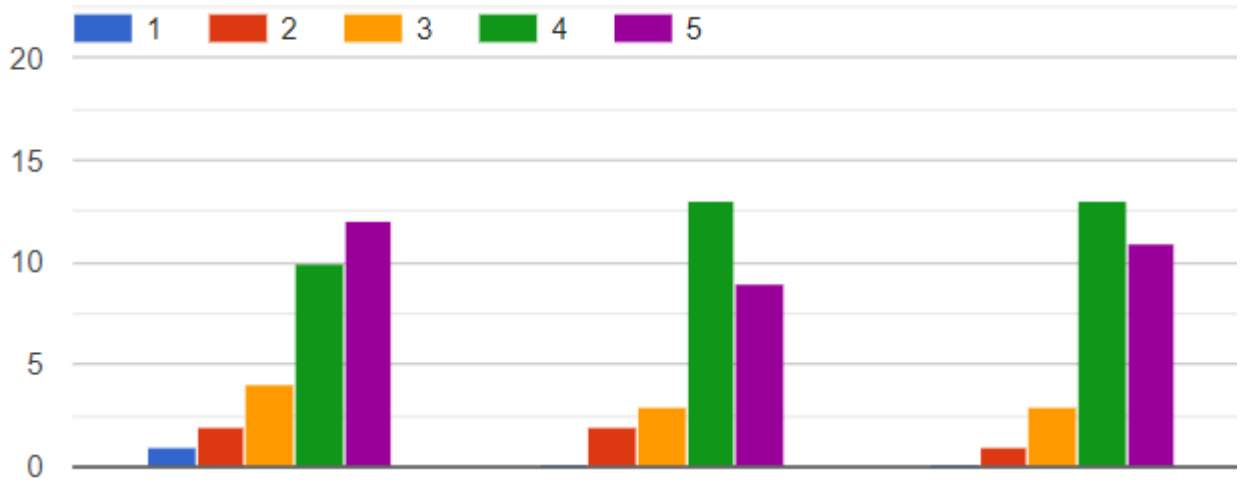
How often do you think you will use the web application?

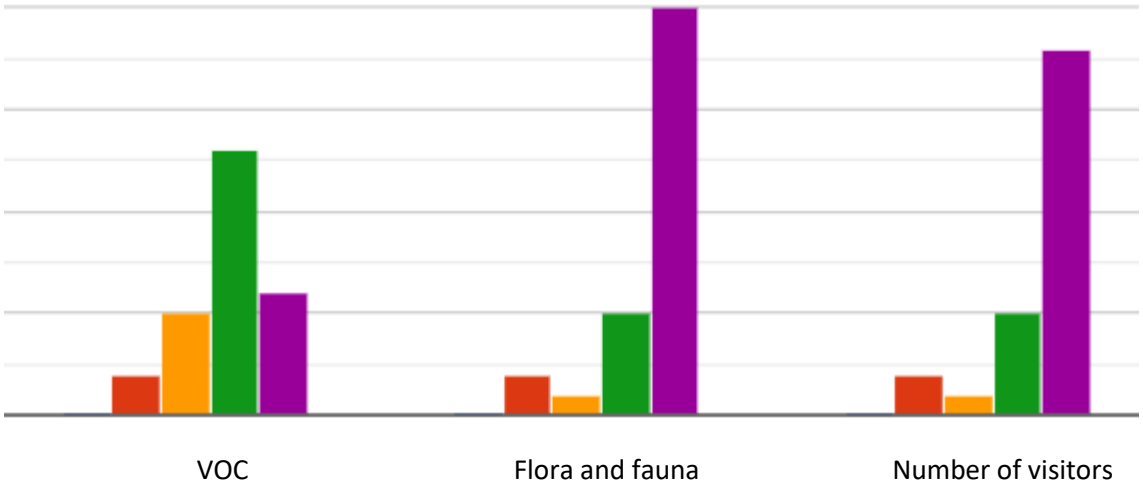
(1 = never again - 5 = very often)



Usefulness of the parameters that are being measured in the pilot

(1 = useless – 5 very useful)





Which other parameters/variables would you like to see measured?

- Noise level in different areas of the park
- Parking spaces
- Wind speed
- Distribution of people within the playground
- UV radiation
- UV radiation

Would you recommend the experience to other users? Why?

- Yes
- You know curiosities about the flora and fauna of the park, which would otherwise be difficult to know
- Interesting
- Yes. It is good to know about the wetland

- Yes, to encourage citizen participation in these type of experiences and not restrict them to the scope of research entities.
- Yes, it is a different way to visit the park
- Definitely
- Yes, since you will get information of interest
- Of course
- The contents are interesting and educational.
- Interesting information
- Yes, it is another way to visit the park

Quantitative evaluation - Specific Key Performance Indicators

To achieve success, KPIs were defined in deliverables D2.2, D2.3 and D2.4 M-Sec pilot's definition, setup and citizen involvement report. The idea is to focus on the domains, areas, fields, and critical factors, and to address the elements that are needed to complete the evaluation the achieved results, so that design, validation, and testing of the M-Sec framework in terms of security provided can be assessed.

The achieved results in UC1 are presented in the table below.

Table 15. UC1 KPIs Results

#KPI	Goal	How to measure?	Target	Achieved
#Participants	Minimum number of end users to test the solution provided	Number of end users registered into the system	≥50 users (1st trial: 10-15 friend users, 2nd trial: 50 participants)	60
#Active users	To evaluate the real activity of registered participants	Connections to the web app	≥50	416
#Data tampered	Verify data reliability (data has not been modified)	Use Blockchain, sensitive data from this use case can be tamper proof. Data will be modified on purpose during lab testing.	0	0
#Unauthorised intents to access to data	Avoid unauthorised users having access to sensitive data	Through smart contracts, it is possible to verify whether someone has authorization or not. Warning logs will be received to alert about it.	0	0

#DDoS attacks	Avoid attempts to disrupt normal traffic	Putting IoT devices on the Internet before going public and evaluating their interactions.	0	0
#Data Theft	Avoid infiltration in the overall M-Sec system and other project resources	Attacks to the IoT devices to get information (not available) and/or access to other elements in the system.	0	0

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

Qualitative evaluation

The qualitative evaluation was addressed through a survey to try to get more in-depth feedback. The survey was elaborated in such a way all the most important aspects of the pilot are covered. In this regard, questions about security, privacy, as well as the implementation of the pilot were included.

Two types of questionnaires have been provided in order to collect feedback and improvement areas during the pilot trial. One for teleoperators from Atenzia in charge of monitoring ageing users and the second one to end users (elder adults). Surveys template conducted can be found on D2.4 M-Sec pilots definition, setup and citizen involvement report – Second version.

Below, the obtained results are presented.

Table 16. UC2 Qualitative Survey conducted to Atenzia

#	Questions	Answer User 1&2
1	What is your role?	Technical Coordinator
2	What is your gender?	Female
3	How easy was Senior Care to use? (From a scale from 1 (very unsatisfied to 5 Very satisfied)	3
4	How would you score the look & feel of the solution provided? (From a scale from 1 (very unsatisfied to 5 Very satisfied)	3
5	Did Senior Care help solve your problem/achieve your goal? (From a scale from 1 (very unsatisfied to 5 Very satisfied)	3
6	How easy was the installation procedure of the home sensors at the user's home? (From a scale from 1 (very unsatisfied to 5 Very satisfied)	3
7	To what extent do you feel safer using the Senior Care system? (Feeling of safety/reliability, acceptance) (From a scale from 1 (very unsatisfied to 5 Very satisfied)	4

#	Questions	Answer User 1&2
8	How well does the Senior Care system complement the existing analogic system to monitor ageing people? (From a scale from 1 (very unsatisfied to 5 Very satisfied)	4
9	How easy is it to detect a non-regular behavior of a user through the alerts system implemented? (From a scale from 1 (very unsatisfied to 5 Very satisfied)	3
10	How reliable do you think the information is provided by the Senior Care system is? (From a scale from 1 (very unsatisfied to 5 Very satisfied)	2
11	How interested would you be in using Senior Care after the end of the test period? (From a scale from 1 (very unsatisfied to 5 Very satisfied)	2
12	According to your personal view, to what extent do you believe that Senior Care and the M-Sec Project can help to reduce the breach about current security concerns in terms of data protection and increase user trust? (From a scale from 1 (very unsatisfied to 5 Very satisfied)	4
13	How concerned would you be about your privacy when using Senior Care? (From a scale from 1 (very concerned to 5 Not at all)	3
14	Compared to the current analogic system used by Atenzia, how would you evaluate the accuracy of Senior Care? (From a scale from 1 (very unsatisfied to 5 Very satisfied)	2
15	Were there any false detections?	No
16	Did you collect any feedback or impressions from the end-users who provided the tip about the following aspects:	

#	Questions	Answer User 1&2
16.a	Do you think that users perceived the security and trustiness on the system?	During the months when the platform worked correctly, users' activity could be monitored, so that any incidents could be detected. Unfortunately, during the second phase, both the platform and the home sensors did not work properly at all.
16.b	Do you think that users found the procedure to test the solution well-explained?	I think so, any incident/doubt... has been tried to be solved.
16.c	What do you think are the main drivers for users to participate in the tele assistance service offered by Atenzia?	The need to feel safer as well as the trust they have in the tele-assistance company (Atenzia) and Santander City Council are the main reasons why they have participated in this pilot.
16.d	Do you think that users will speak about it with friends and relatives about this particular pilot testing Senior Care?	We believe that yes. At some point they will talk about the home sensors and the monitoring of their activity in their home through these devices.
17	Lessons Learned:	-
17.a	What worked well	No feedback provided
17.b	What didn't work so well?	Bed occupancy sensors have not worked properly from the begining of the pilot. In these last few months, we have had problems with the platform: it does not provide data on the activity of the sensors, and it is very difficult to monitor users correctly.
17.c	What is still needed to make the solution more interesting for Atenzia? (e.g., new functionalities?	A statistics module to extract data in excel format in a more detailed way by user, by type of sensor, date, etc.

#	Questions	Answer User 1&2
18	How would you assess the collaboration with Worldline as the technical partner provider of Senior Care? (From a scale from 1 (very unsatisfied to 5 Very satisfied)	3
19	Please, rate your overall satisfaction with the solution itself, the technical support, and the M-Sec contribution in terms of security. (From a scale from 1 (very unsatisfied to 5 Very satisfied)	3
20	Comment Box (Here you can provide any additional feedback or clarifications you may have on the answers)	No feedback provided

Table 17. UC2 Qualitative Survey conducted to end users

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

Quantitative evaluation - Specific Key Performance Indicators

To achieve success, KPIs were defined in deliverables D2.2, D2.3 and D2.4 M-Sec pilot's definition, setup and citizen involvement report. The idea is to focus on the domains, areas, fields, and critical factors, and to

address the elements that are needed to complete the evaluation the achieved results, so that design, validation, and testing of the M-Sec framework in terms of security provided can be assessed.

Below, the results achieved in UC2 are presented.

Table 18. UC2 KPIs Results

#KPI	Goal	How to measure?	Target	Achieved
#Participants	Minimum number of end users to test the solution provided.	Number of end users (ageing people) registered into the system	≥5 users	5
#Daily Home Activity Data	To evaluate the volume of data generated and its scalability.	Raw data sent from the Home IoT sensors to Senior Care	<1GB	78MB
#Data speed	To evaluate speed at which new data travels	Latency time	≤25s	<5s
#Events that have occurred during the length of the pilot	In order to have a minimum sample where to verify reliability	Statistics Module	>100	221.023
#Alarms that have been handled during the length of the pilot	To evaluate the reliability of the alarms raised	Statistics Module	≥ 60 (4 alarms/month per user)	277
#Data tampered	Verify data has not been modified	Thanks to Blockchain, sensitive data from this use case can be tamper proof due a hash pointer. The hash will indicate whether data has been modified.	<3 Attempts / <3 Detections	0
#Unauthorised intents to access to data	Avoid unauthorised users have access to sensitive data	Through smart contracts, it is possible to verify whether someone has authorization or not. Warning logs will be received to alert about it.	<3 Attempts / <3 Detections	0
#Data exchanged	To evaluate the business value of the anonymized data sent	Datasets sent to the marketplace (1 dataset per sensor registered).	>20	>20

#KPI	Goal	How to measure?	Target	Achieved
	from Senior Care to the M-Sec Marketplace			
#false positive events	Verify the reliability of the sensors	Manual way by verifying the reliability of the data with the end user	<5	52
#End points accessed	Higher number of end points higher vulnerability grade	Access log file	<10	20 Module MQTT has 2 in order to check the status and let data be added to the system. Module scheduler has 1 to provide an entry point for the marketplace. The Security & Storage Functional Group API is not specific from UC2, (has 14). 3 external.

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

Qualitative evaluation

The qualitative evaluation survey was not conducted for use case 3 because this use case only focuses on providing the security element for the KEIO Mobile Sensing Platform. Due to extensive technical nature and security knowledge, the citizens or non-technical stakeholders were not a part of this use case. Therefore, unlike other use cases, the use case 3 focused on the quantitative evaluation only.

Quantitative evaluation - Specific Key Performance Indicators

In Use case 3, the Keio Mobile Sensing Platform is being used to collect more than 50 kinds of data. This evaluation was conducted in two stages. The first stage was evaluated from Dec. 1 to 30, in 2020. The gaps were mitigated and tested in the second stage from July 15 to September 30, 2021. From the evaluation, we obtained both security and non-security results regarding the KPIs. These results validate that the mobile sensing platform was functioning well, and its security was properly ensured.

In the following table, we summarized the quantitative evaluation results:

Table 19. UC3 KPIs Results

#KPI	Goal	How to measure?	Target	Achieved Value
# platform users	Having multiple common platform users as a secure and trustworthiness mobile sensing platform.	Number of platform users	3	10 garbage truck sensing SmileCityReport Restaurant environment sensing class room environment sensing outside environment sensing public Bus environment sensing MinaRepo Sight Seeing Area sensing Amusement Park sensing Sensorizer
# Anonymization	Functional verification of privacy data protection	Number of privacy data erased from	More than 20 transactions	2 GANonymizer Also used in

#KPI	Goal	How to measure?	Target	Achieved Value
		video data as privacy data protection	privacy-related objects	SmileCityReport app. service
# Secure Data Processing	Securely distributes data as a Secure Trustworthiness mobile sensing platform.	Number of data safely delivered as Secure Trustworthiness mobile sensing platform	More than 50 kinds of data	More than 50 11 kinds of data from garbage truck sensing, 8 kinds of data from SmileCityReport 4 kinds of data from Restaurant environment sensing 4 kinds of data from class room environment sensing 4 kinds of data from outside environment sensing 4 kinds of data from public Bus environment sensing 5 kinds of data from MinaRepo 2 kinds of data from Sight Seeing Area sensing 2 kinds of data from Amusement Park sensing more than 10 kinds by Sensorizer (Weather, River water level, precipitation amount, traffic jam,.....)
"Scan attempts blocked"	Hackers frequently scan the internet to find open ports or services available on a device before an attack. Blocking scan can help reduce the attack surface.	Using the security monitoring tool	90% or more	100%

#KPI	Goal	How to measure?	Target	Achieved Value
Ping/ICMP packets blocked	Hackers need to know the IP address of their target for which they commonly use Ping/ICMP packets. Blocking this can make it difficult for them to pinpoint an attack	Using the security monitoring tool	90% or more	100%
Telnet access blocked	Telnet service is one of the highest exploited service for breaking into a device remotely. Blocking it would avoid such attacks.	Using the security monitoring tool	90% or more	100%
SSH access blocked	SSH is another service that is commonly under attack to gain remote access to the controls.	Using the security monitoring tool	90% or more	100%
Misc. attacks blocked	There are many kinds of attacks conducted by various bad actors that are flagged by the threat intelligence communities. IDS/IPS can summarize various attacks based on their signature to block them from succeeding. This will help the solution to block any such flagged attacks.	Using the security monitoring tool	90% or more	100%

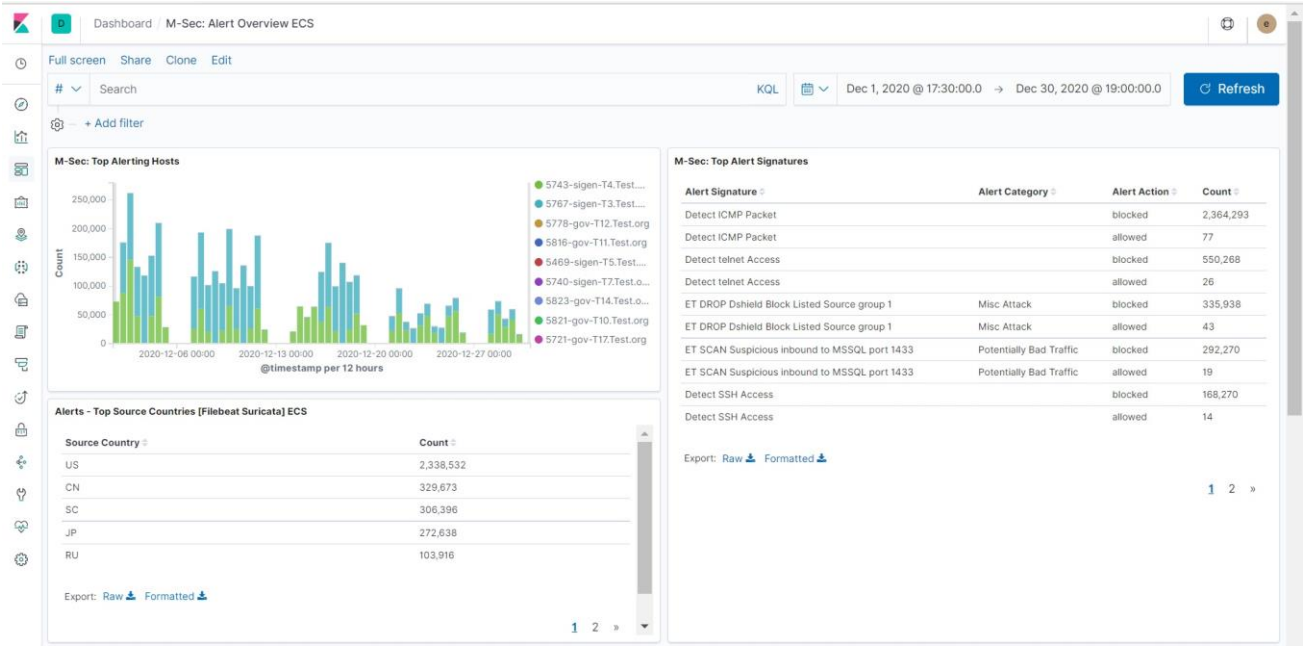


Figure 18: UC3 Pilot: Stage-1 Results

Figure 18 shows the results at stage-1 of UC3 pilot. Further improvements were made in stage-2. As described in the deliverable (D4.2), a new security component (Stealth Security) was introduced to address the unknown attacks by hiding the ports stealthily so that no intelligence or response can be collected by the attackers. The IoT gateway device becomes invisible on the Internet and only allows authorized users with correct sequence of specific secret knocks. A research paper on this has been published in the vol.29 of Journal of Information Processing [2]. The results of improvement are shown in Figure 19.

[2] Bokhari, A.H., Inoue, Y., Kato, S., Yoshioka, K., and Matsumoto, T.: Empirical Analysis of Security and Power-Saving Features of Port Knocking Technique Applied to an IoT Device. Journal of Information Processing, Vol.29, pp.572-580 (2021). DOI: 10.2197/ipsjjip.29.572

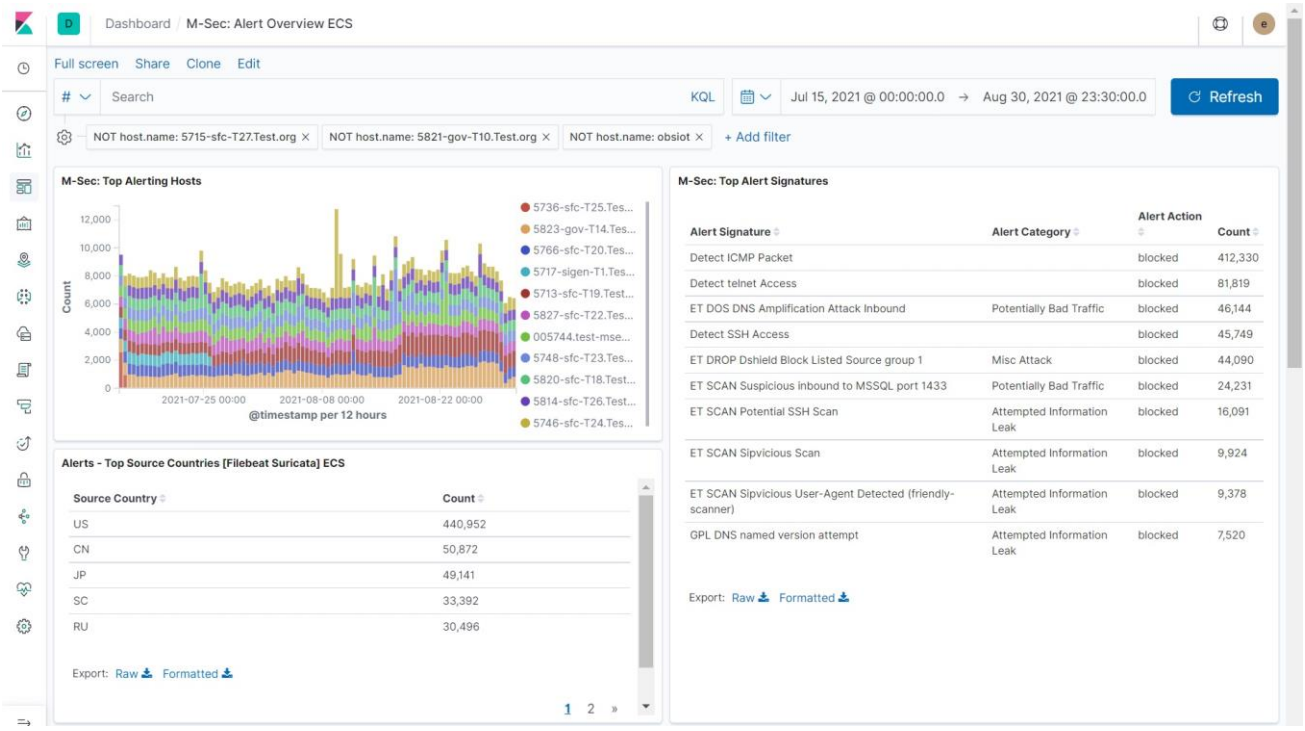


Figure 19: UC3 Pilot: Stage-2 Results

As can be seen in the “graph” and “count” statistics, the suspicious traffic has been blocked 100% and the overall number of attempts (Scans, ICMP/ping, Telnet, SSH, Misc. Attacks) has also been reduced effectively compared to the stage-1 results. The data from sensors has been received securely without any issue or interruption, enabling the trust on the Secured Keio Mobile Sensing Platform.

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

Qualitative evaluation

The mechanism to filter privacy-related objects is applied, in the Smile City Report application, to persons, cars, and bikes. With help of this mechanism images were anonymized successfully as shown in the following picture. This picture was taken in a Ramen restaurant in Fujisawa where two persons exist. One of them is made completely transparent while the other is half-visible. Such a half-anonymous case was seen in the pilot when just a half of a person is included in a picture. Also, there were cases where objects, which are not privacy-related, were anonymized. This is since those objects are similar to one of the privacy-related objects learned by AI in some sense.

Figure 20: Screenshot from the Smile City Report

Quantitative evaluation - Specific Key Performance Indicators

To achieve success, KPIs were defined in deliverables D2.2, D2.3 and D2.4 M-Sec pilot's definition, setup and citizen involvement report. The idea is to focus on the domains, areas, fields, and critical factors, and to address the elements that are needed to complete the evaluation the achieved results, so that design, validation, and testing of the M-Sec framework in terms of security provided can be assessed.

The achieved results in UC4 are presented in the table below.

Table 20. UC4 KPIs Results

#KPI	Goal	How to measure?	Target	Achieved Value
# of privacy-related objects filtered out from input images	To evaluate the volume of data from which privacy-related objects have been filtered out	Counting the number of processed images in the component.	More than 70% of the objects that the filtering component originally targeted.	More than 70%
# of objects going to SecureSOXFire	To evaluate how much data objects to be input into the public smart city network	Number of data (post object)	100	1,466 (# of posts in PHASE2 and PHASE 3)

Cross-border

In this pilot, users are asked to post pictures according to a topic specified by the Smile City Report application. They can also post comments to other posts. During the cross-border execution of this pilot, internationalization of the comments, i.e., Spanish-Japanese translation, was the key to achieve mutual understanding of the scene behind the images. In the following picture, the Spanish comment “al rico helado” is translated into Japanese “濃厚なアイスクリームに.”

Figure 21: Cross border use of the Smile City Report

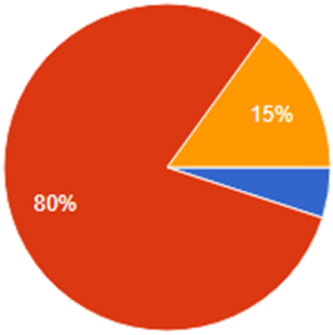
The qualitative evaluation was addressed through an online survey, in Japanese and Spanish depending on the city, to try to get more in-depth feedback. The survey was elaborated in such a way all the most important aspects of the pilot are covered. In this regard, questions about security, privacy, as well as Smiley City Report app and functionalities were included. The survey was implemented with the Google Forms service, and the link to the survey was included in the Smile City Report application. Field trial participants were invited to fill in this online survey, once they get 3,000 points while using the Smile City Report app, as detailed in D2.4 M-Sec pilots definition, setup and citizen involvement report – Second version, survey template is also available.

The following table shows the questions and answers of the 20 participants from Santander in the cross-border pilot.

Table 21. UC4 Cross-border Qualitative Evaluations Survey in Santander

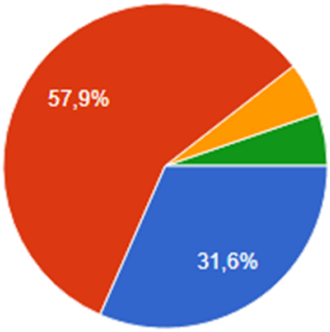
User profile


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



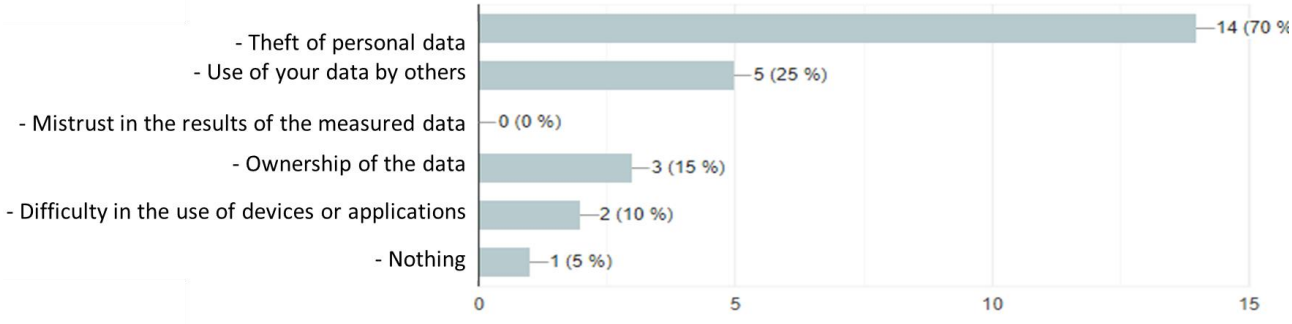
- I am fully aware (i.e. I always read carefully the data protection policies when using a given device or application)
- I am not that fully aware (i.e. I do not always carefully read the data protection policies when using a given IoT device or application)
- I am not aware (i.e. I never read and always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

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

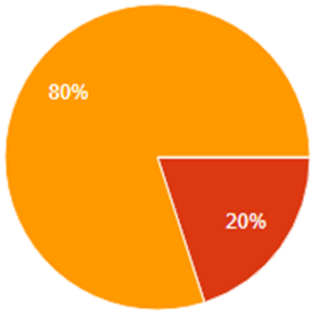


- I go and check carefully the data protection policies when using the IoT device or application
- I stop using that specific IoT device or application
- I do nothing
- Nothing

What are your concerns when using IoT devices or applications?



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

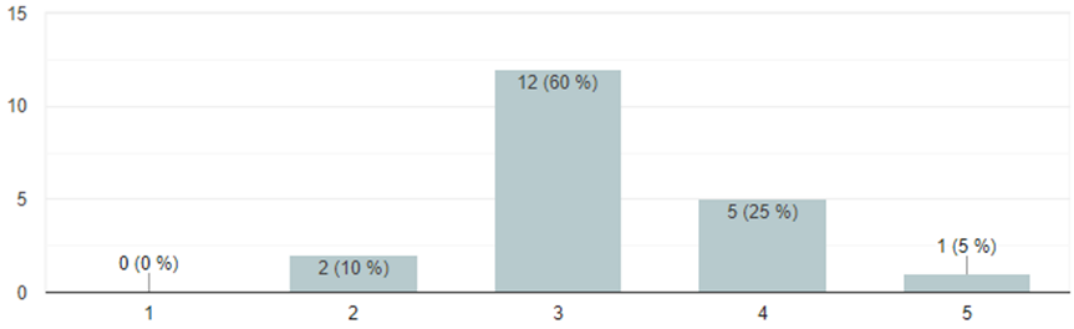


- No, as I am not from an EU country
- Yes, I am completely aware
- I have heard about it but I am not completely aware of my rights
- No

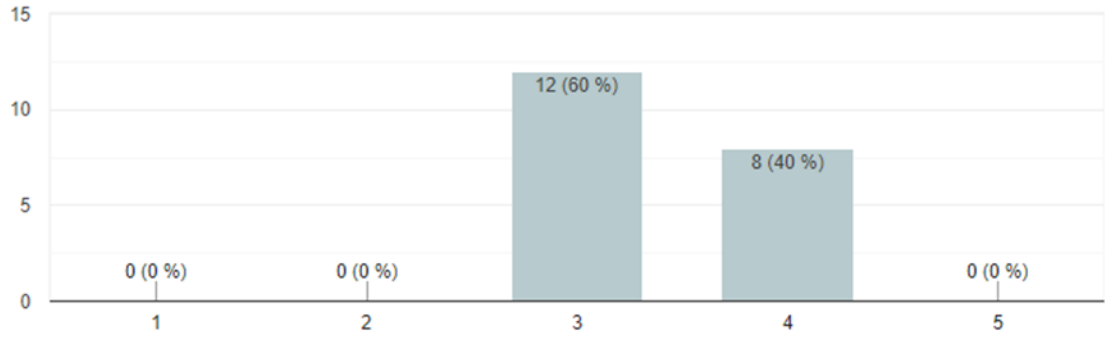
Are you aware of your rights regarding Japan's Act on the Protection of Personal Information (APPI)?

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

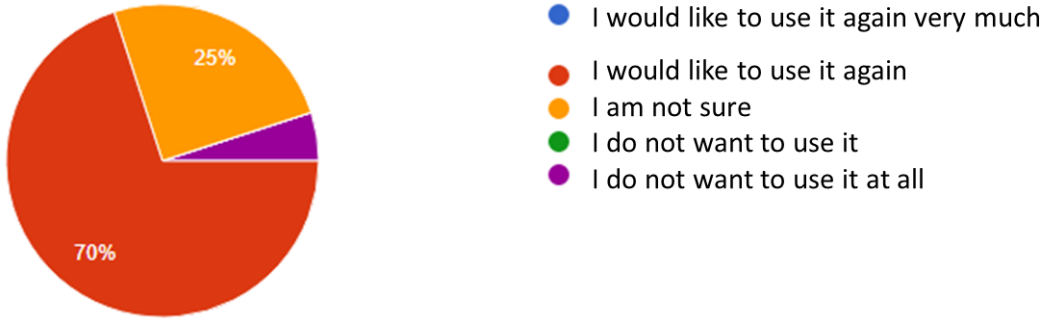
How did you like Smile City Report app? (1 Not satisfied at all – 5 Very Satisfied)



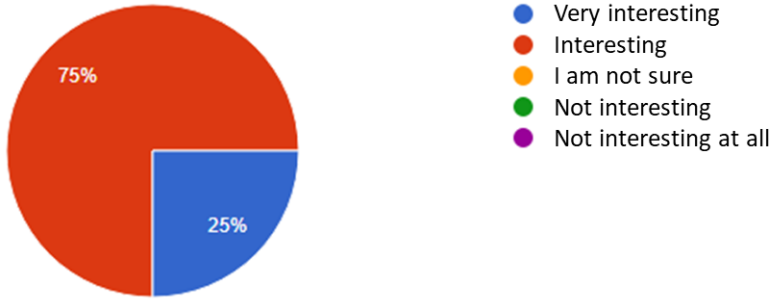
Were there any post that are valuable for you? (1 Not at all – 5 Many)



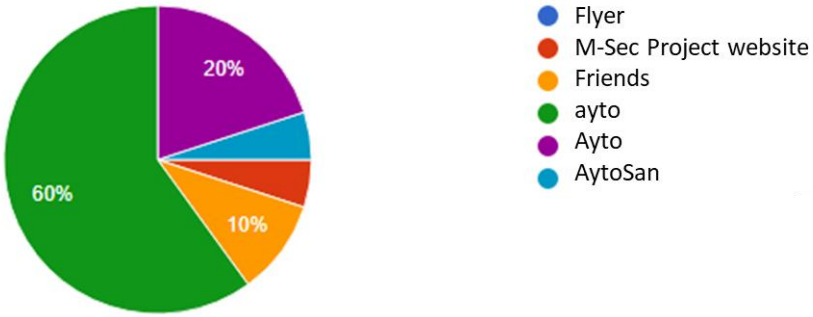
How was the app that "posts according to the theme" about the current state of the city? Do you want to use this app again?



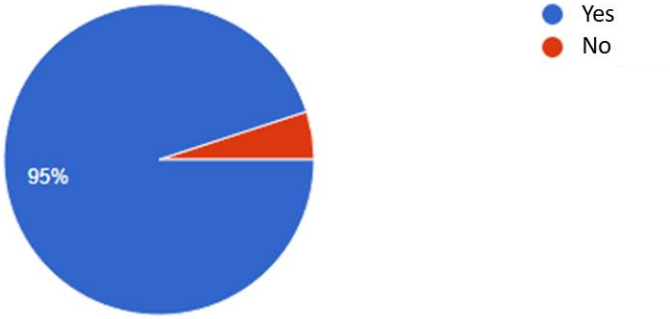
How was the function to take pictures of the scenery and yourself at the same time with the two cameras on your smartphone?



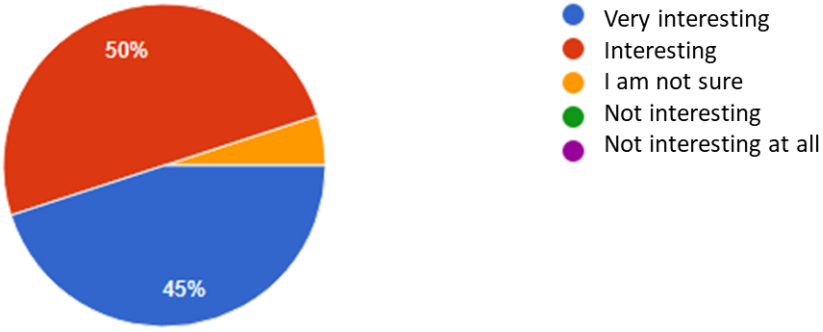
How did you know the Smile City Report app?



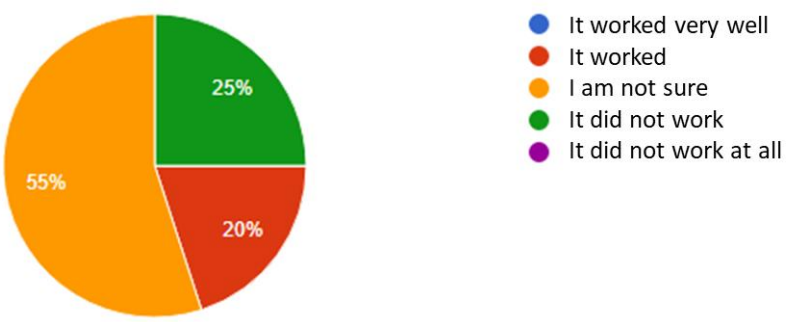
Did you use a privacy protection tool called "GANonimizer" in the app? It is an AI technology to erase the reflected "parts that may contain privacy information" in the picture such as people.



How did you think about the tool?



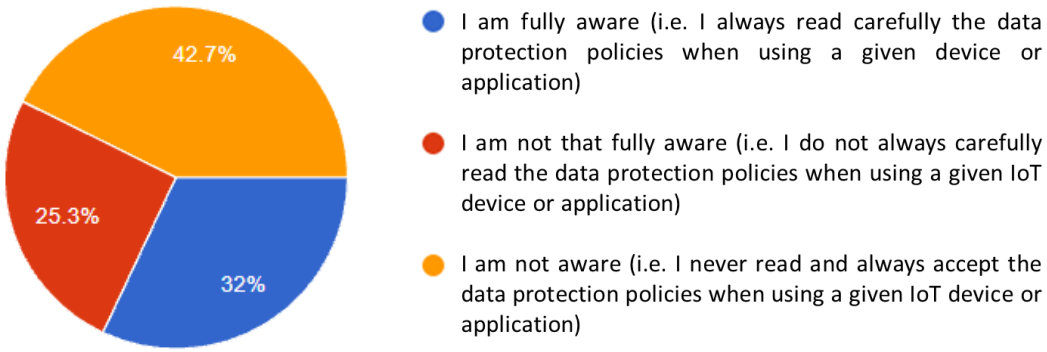
Did the privacy protection tool properly remove the "parts that would contain privacy information" from the photo, such as people?



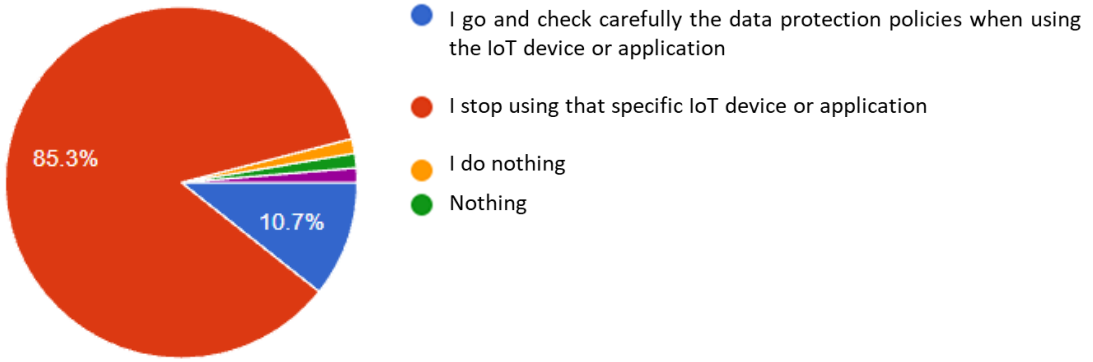
The following table shows the questions and answers of the participants from Fujisawa.

Table 22. UC4 Cross-border Qualitative Evaluations Survey in Fujisawa

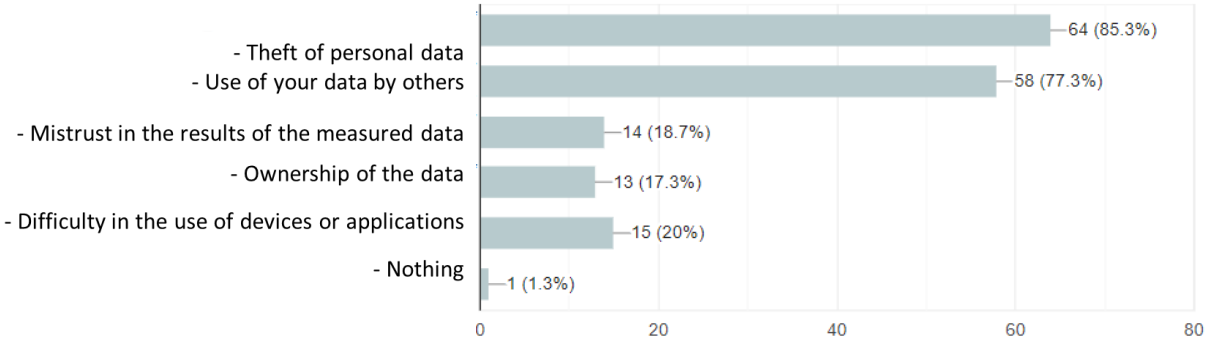
User profile


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


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

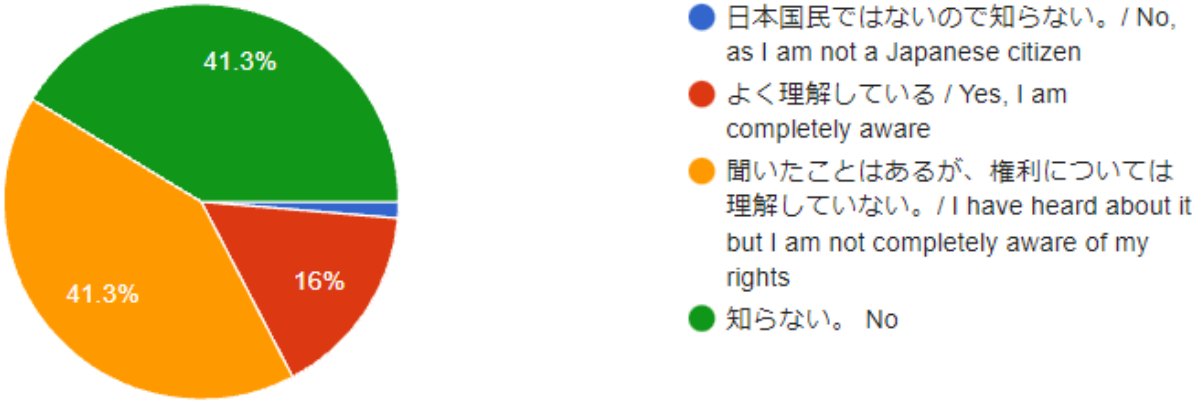


What are your concerns when using IoT devices or applications?

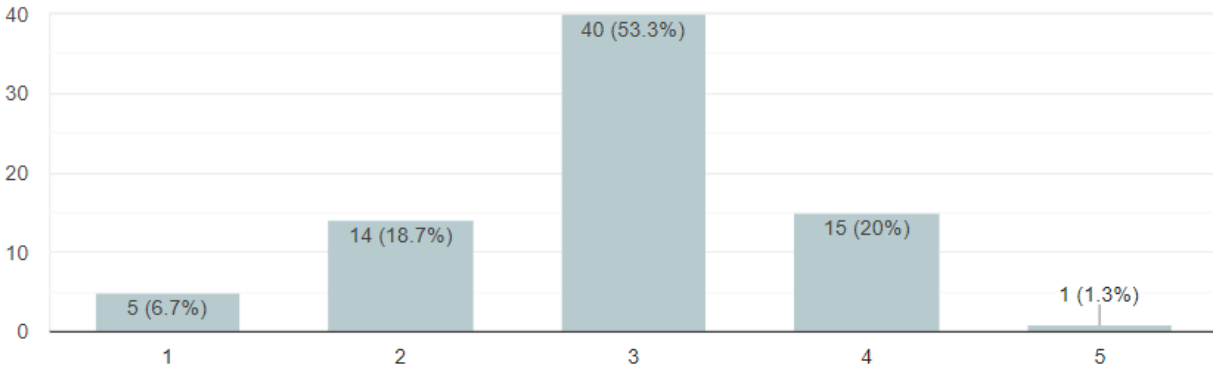


Are you aware of your rights regarding EU's General Data Protection Regulation (GDPR)?

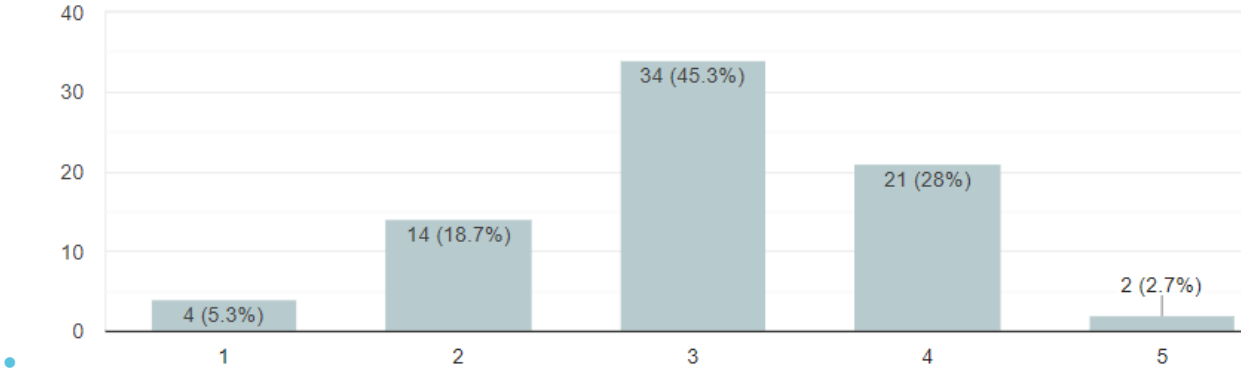
Are you aware of your rights regarding Japan's Act on the Protection of Personal Information (APPI)?



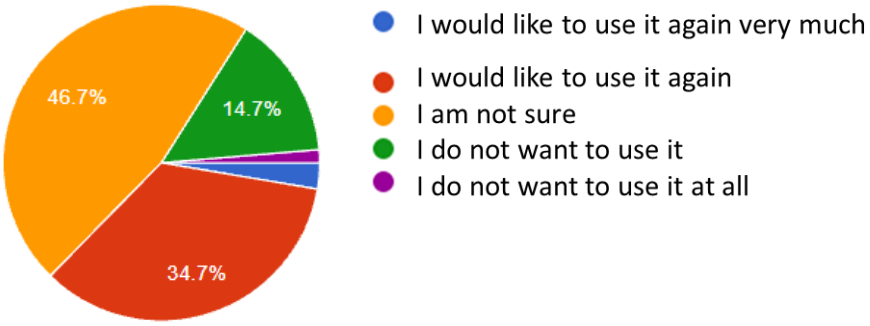
How did you like Smile City Report app? (1 Not satisfied at all – 5 Very Satisfied)



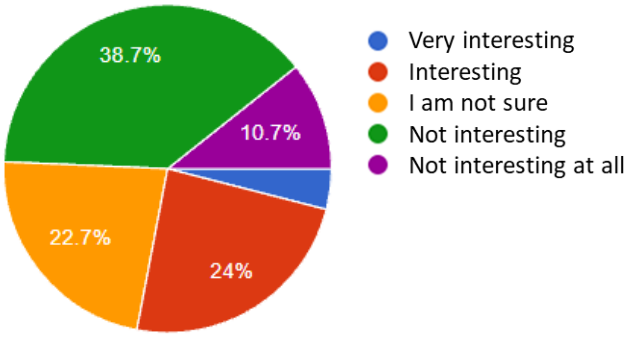
Were there any posts that are valuable for you? (1 Not at all – 5 Many)



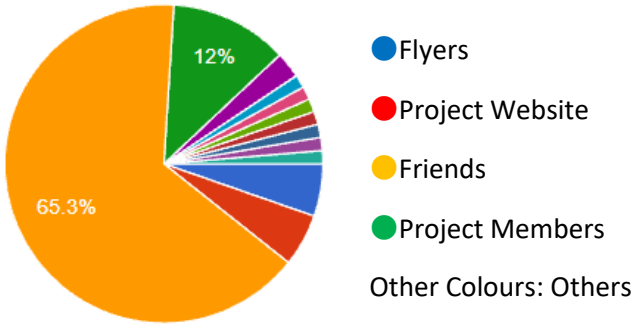
How was the app that "posts according to the theme" about the current state of the city? Do you want to use this app again?



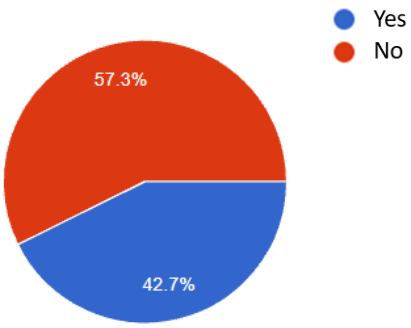
How was the function to take pictures of the scenery and yourself at the same time with the two cameras on your smartphone?



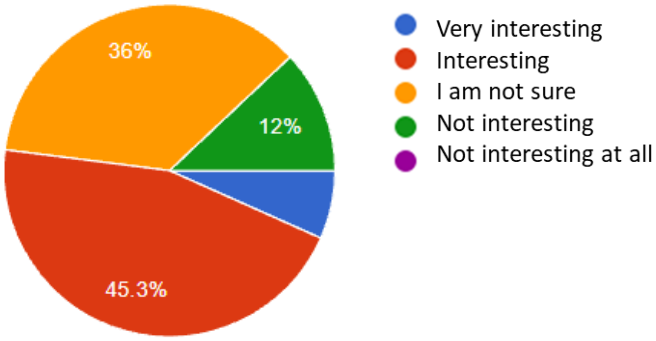
How did you know the Smile City Report app?



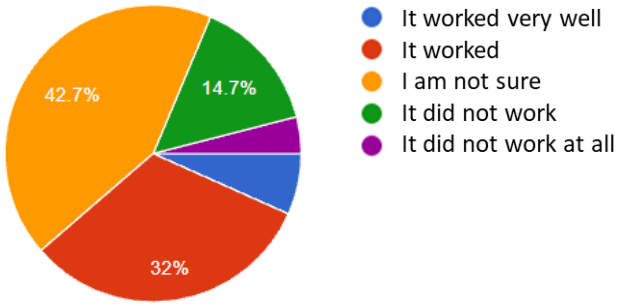
Did you use a privacy protection tool called "GaNonimizer" in the app? It is an AI technology to erase the reflected "parts that may contain privacy information" in the picture such as people.



How did you think about the tool?



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



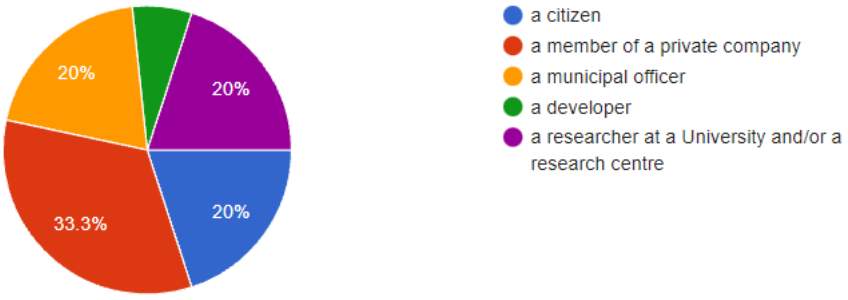
3.6 Pilot 5 (Use case 5): Smart City Data Marketplace with secure Multi-layer Technologies

Qualitative evaluation

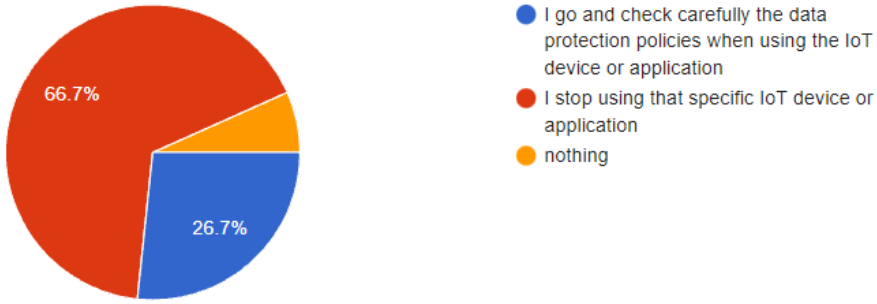
The qualitative evaluation was addressed through a user survey to try to get more in-depth feedback. The survey was elaborated in such a way that all the most important aspects of the pilot are covered. In this regard, questions about security, privacy, as well as the implementation of the pilot were included. Besides, the language was adapted to avoid too complex questions that might lead to unusable responses.

The survey was implemented with the Google Forms service, a web application that allows the fast and easy creation of surveys. The table below includes answers from European and Japanese citizens.

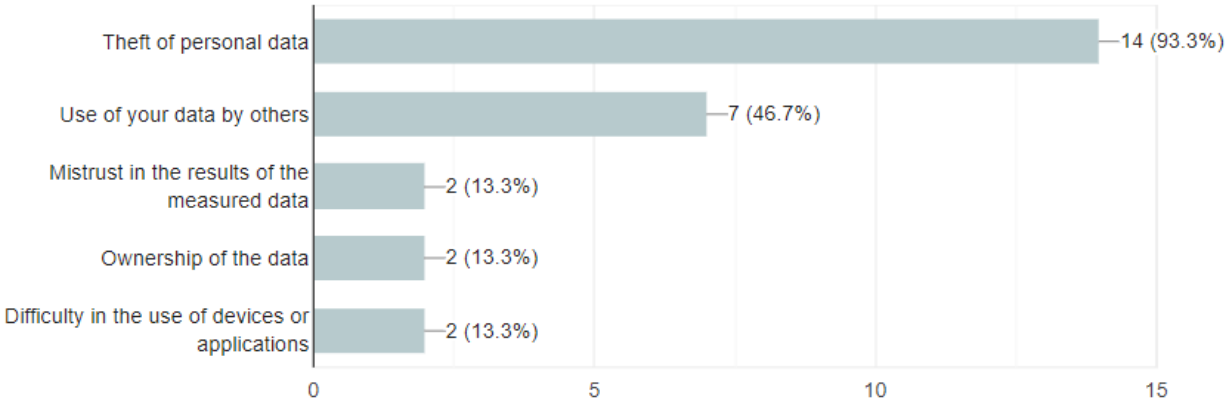
Table 23. UC5 Crossborder Qualitative Evaluations Survey in EU and Japan

User profile

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

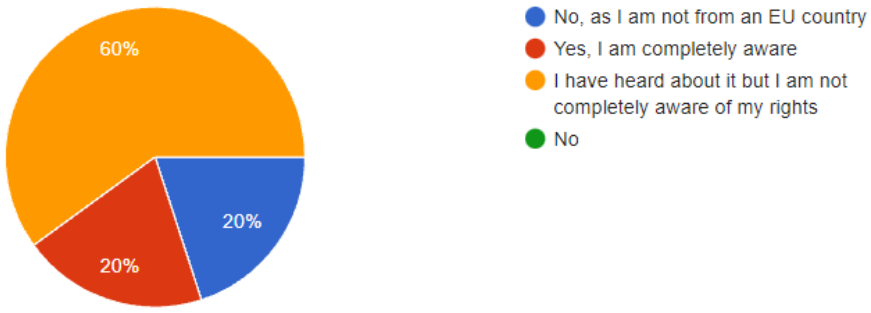
What are your concerns when you hear about a cyber-attack in a given IoT device or application that you are currently using?



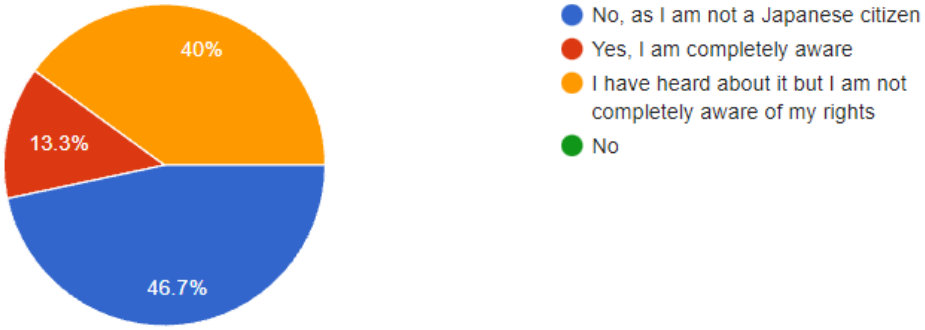
What are your concerns when using IoT devices or applications?



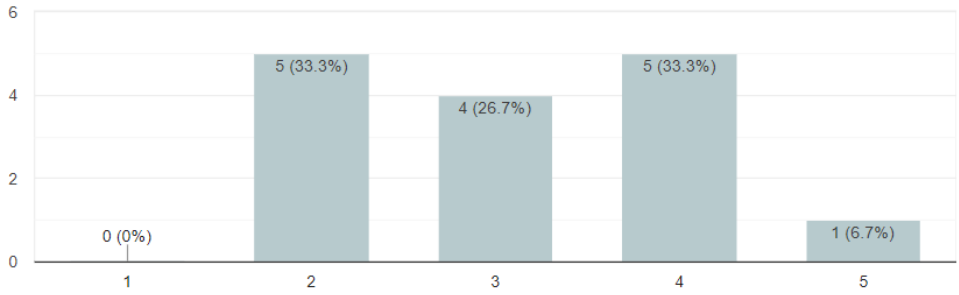
Are you aware of your rights regarding EU's General Data Protection Regulation (GDPR)?



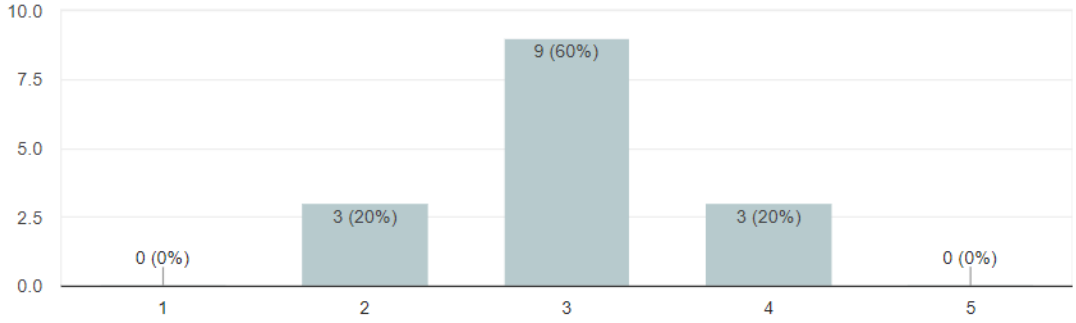
Are you aware of your rights regarding Japan's Act on the Protection of Personal Information (APPI)?



Do you think that the marketplace is user-friendly? (1 Not satisfied at all – 5 Very Satisfied)

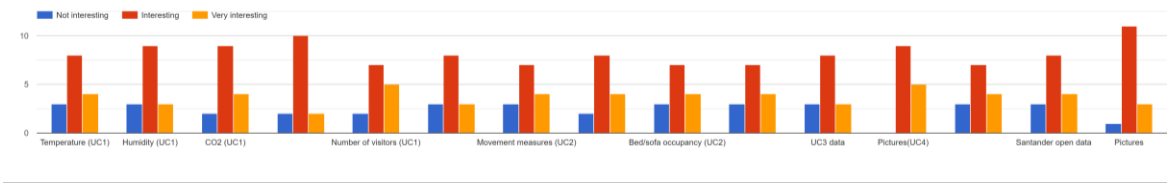


How often do you think you will use the marketplace? (1 Not at all – 5 Many)

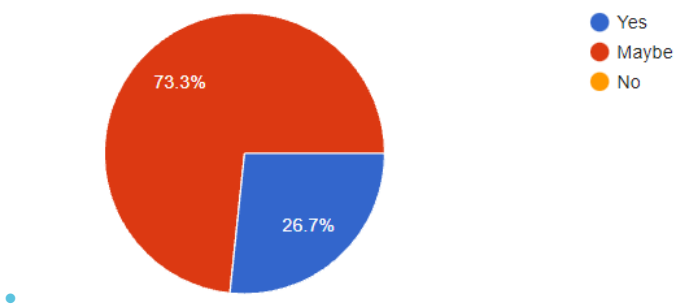


Please rate the data available in the marketplace according to your interest.

※The data was interesting for all users.



Would you recommend Marketplace to other users?



Quantitative evaluation - Specific Key Performance Indicators

In the context of Pilot 5 different KPIs were achieved, as shown in the following table:

Table 24. UC5 KPIs Results

#KPI	Goal	How to measure?	Target	Achieved Value
Total exchange of virtual currencies for virtual goods trade via the marketplace	Have a total exchange of 10000 units	Measuring the participation and activity in the Marketplace	10000	40860
Number of peer nodes sustaining the blockchain during the operation of the pilots	6 nodes	Measure the total number of nodes	6	115
Number of blockchain implementations piloted for the purposes of use cases	2	Measuring the different implementations	>2	2
Smart objects joining in the marketplace	1000	Measuring the activity in the IoT Marketplace	1000	2,829

Cross-border

In the previous subsection, the table provides figures and details about the overall cross border activity. Within the context of M-Sec, in “UC5 – Smart City Data Marketplace with Secure Multi-Layer Technologies”, the consortium focused on building an M-Sec marketplace where data collected during field trials in each UC could be traded in both Japan and Europe while ensuring security on all layers. Users were able to connect and use IoT Marketplace, purchase sensor data and take advantage in different supported features without any geographic limitation.

As an indicative example, there were more than 40.000 exchanges of virtual currencies for virtual goods trade in the marketplace by registered users from different countries. Of course, it is not feasible to distinguish the location of users, since no personal data are kept.

4. Cross-border replication

Below two ideas for two additional future cross-border UCs are considered, to demonstrate the replicability of the M-Sec solutions.

4.1 SmileCityReport new theme for city events

In the initial planning of the cross-border use cases, the plan was to participate in a gastronomic event as the "Choi-nomi" Drinking Festival, held twice a year in Fujisawa City in May and November, and at the same time holding a similar gastronomic event in Santander, to share the photos of the event to see the popular food, drinks and the people getting merry in each city.

Also, a virtual sightseeing event was planned, as the gastronomic events were not held because of the pandemic situation, to enjoy the feeling of traveling even in the pandemic situation.

The events mentioned above can be held in any cities in the world and so it can be thought to be replicated anywhere.

4.2 Marketplace for data, APIs and microservices

Within the context of M-Sec, in “UC5 – Smart City Data Marketplace with Secure Multi-Layer Technologies”, the consortium focused on building an M-Sec marketplace where data collected during field trials in each UC could be traded in both Japan and Europe while ensuring security on all layers. The high-level objective was to enable an open and dependable ecosystem of Smart City data-providers and consumers which would operate in a reliable, sustainable, and, most importantly, secure manner. Our vision is for this ecosystem to, eventually, give rise to a strengthened European and Japan ICT industry and academia able to meet key societal and economical needs. From a more practical point of view, the consortium focused on innovation related to the design and development of an IoT Marketplace that will match the supply and demand of Smart City datasets. A permissioned blockchain infrastructure was used for facilitating several use cases, and the corresponding supporting middleware was developed to enhance the marketplace with several capabilities with security mechanisms and smart contracts.

The business model, technical development, and cross-border users’ engagement achieved in this UC could be replicated and extended in a similar scenario: instead of focusing on an IoT-datasets marketplace, it could be possible to provide in the future an IoT Marketplace for data but also for APIs and for microservices. An indicative example of an APIs Marketplace is RapidAPI Hub[3]. Such an extension would considerably enhance the development capabilities of interested parties and would naturally have a cross-border nature.

[3] https://website.rapidapi.com/?site

5. Conclusions

This document provides a report on the validation and overall evaluation of the M-Sec ecosystem. The report explains the technical tests that have been carried out during the validations process, as well as the assessment of the Key Performance Indicators and the feedback from M-Sec users.

Firstly, the report provides the final view on requirements and security threats mitigation. In this regard, the document shows that 131 out of 139 requirements were covered at 100% level, while the other 8 requirements were considered obsolete (6 out of 8) or less relevant (the other 2). Besides, the 72 security threats that were considered to apply to M-Sec were mitigated at 100% level.

Secondly, the deliverable provides the assessment of the Key Performance Indicators from a general point of view, as well as the Use Case specific Key Performance Indicators. All the indicators were evaluated, resulting in the achievement of all the goals/targets.

Finally, the feedback from users were obtained through online consultations and UC-specific surveys. This action involved the interaction with hundreds of users and interested citizens from Europe and Japan. The valuable information that has been obtained will be the first step towards the further development and potential replication of project results.