



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

D5.8: Market Analysis and Exploitation – 3rd year

September 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 | D5.8 Market Analysis and Exploitation - third year report |
| Work Package | WP5 |
| Submission date | September 2021 |
| Deliverable lead | WLI/NTTDMC |
| Authors | WLI, ICCS, CEA, F6S, TST, SAN MUN, NTTE, KEIO, YNU, NII, WU, NTTDMC |
| Internal reviewer | ICCS/NTTE |
| Dissemination Level | Public |
| Type of deliverable | R |

Worldline



YNU



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 (Organisation) | Changes |
|-------|-------------------|---------------------------|---|
| V0.1 | 26 March 2021 | WLI | Table of Contents, Full Draft. |
| V0.2 | 3 August 2021 | WLI | Included contributions from partners; Individual Exploitation Plans, UC's Driven Exploitation and Components Sustainability. |
| V0.3 | 11 August 2021 | WLI | Contributed to different sections. |
| V0.4 | 17 August 2021 | WLI | Updated Sections 3.1 Market Overview, Section 4 M-Sec Value Proposition & Stakeholders. |
| V0.5 | 20 August 2021 | F6S | Updated Section 6 Marketing Strategy. |
| V0.6 | 24 August 2021 | F6S | Updated Section 6 Marketing Strategy. |
| V0.7 | 25 August 2021 | NTTDMC | Updated Sections 3.2 Competitive Landscape, 5.1 Individual Exploitation Partner's Plan (NTTDMC). |
| V0.8 | 25 August 2021 | WU | Updated Section 5.1 Individual Exploitation Partner's Plan. |
| V0.9 | 25 August 2021 | CEA | Updated Section 2.2 (CEA components license), 5.1 (Individual Exploitation Partner's Plan-CEA) & 5.6 (CEA Components sustainability). |
| V0.10 | 25 August 2021 | WLI | Updated Section 5.1 and 5.6 with the input from NII. |
| V0.11 | 26 August 2021 | KEIO | Updated Section 5.1 Individual Exploitation Partner's Plan. |
| V0.12 | 17 August 2021 | KEIO | Updated minor missing part. |
| V0.13 | 1 September 2021 | ICCS | Provided input in section 5.1 and 5.6. |
| V0.14 | 8 September 2021 | WLI | Reviewed and updated the whole document. |
| V0.15 | 9 September 2021 | KEIO | Updated based on review comment. |
| V0.16 | 9 September 2021 | WLI | Reviewed and updated the whole document. |
| V0.17 | 14 September 2021 | ICCS | Updated Section 2. Reviewed the whole document. |
| V0.18 | 27 September 2021 | YNU | Updated Section 5.1.11 and other minor edits |
| V0.19 | 27 September 2021 | NTTDMC | Updated section 3.2 competitive landscape |
| V0.20 | 27 September 2021 | WLI | Answered review comments |
| V0.21 | 29 September 2021 | NTTE | Reviewed and add some comments |
| V0.22 | 29 September 2021 | WLI | Answered comments and final review. |
| V0.23 | 30 September 2021 | ICCS | Minor changes in Section 2.3. |
| V1.0 | 30 September 2021 | WLI | Ready for submission |





Table of Contents

| | |
|--|----|
| Version history..... | 3 |
| Table of Contents | 4 |
| List of Tables | 7 |
| List of Figures..... | 8 |
| Glossary | 10 |
| 1. Introduction and scope..... | 12 |
| 1.1 Introduction | 12 |
| 1.2 Relation to other WPs and Tasks..... | 12 |
| 2. M-Sec Overview | 14 |
| 2.1 What is M-Sec..... | 14 |
| 2.2 M-Sec Key Solutions Components..... | 18 |
| 2.3 Main differences between M-Sec Project and BigClouT Project..... | 22 |
| 3. Updates on the Market Size & Competitive Landscape | 25 |
| 3.1 Market Overview | 25 |
| 3.2 Competitive Landscape | 26 |
| 4. M-Sec Value Proposition & Relevant Stakeholders | 33 |
| 4.1 Smart Cities..... | 33 |
| 4.1.1 Customer Profile..... | 34 |
| 4.1.2 Product | 34 |
| 4.1.3 Main Value Proposition & Benefits | 35 |
| 4.2 Developers Community | 35 |
| 4.2.1 Customer Profile..... | 35 |
| 4.2.2 Product | 36 |
| 4.2.3 Main Value Proposition & Benefits | 36 |
| 4.3 Citizens..... | 36 |
| 4.3.1 Customer Profile..... | 37 |
| 4.3.2 Product | 37 |
| 4.3.3 Main Value Proposition & Benefits | 38 |
| 4.4 IoT Technology Providers | 38 |
| 4.4.1 Customer Profile | 38 |





| | | |
|--------|---|----|
| 4.4.2 | Product | 39 |
| 4.4.3 | Main Value Proposition & Benefits | 39 |
| 4.5 | Research Institutes & Universities..... | 40 |
| 4.5.1 | Customer Profile..... | 40 |
| 4.5.2 | Product | 40 |
| 4.5.3 | Main Value Proposition & Benefits | 41 |
| 4.6 | M-Sec overall Value Proposition | 41 |
| 5. | M-Sec Exploitation and Sustainability Strategy | 45 |
| 5.1 | Partners' Individual Exploitation Plans..... | 45 |
| 5.1.1 | Worldline | 47 |
| 5.1.2 | ICCS..... | 49 |
| 5.1.3 | Ayuntamiento Santander | 51 |
| 5.1.4 | TST | 53 |
| 5.1.5 | CEA..... | 55 |
| 5.1.6 | F6S | 57 |
| 5.1.7 | NTTE..... | 59 |
| 5.1.8 | KEIO | 60 |
| 5.1.9 | NTTDMC..... | 62 |
| 5.1.10 | WU | 64 |
| 5.1.11 | YNU | 65 |
| 5.1.12 | NII..... | 67 |
| 5.2 | Joint Exploitation | 69 |
| 5.3 | UCs driven Exploitation | 73 |
| 5.3.1 | UC1: Secured IoT Devices to enrich strolls across Smart City Park | 73 |
| 5.3.2 | UC2: Home Monitoring Security System for ageing people..... | 76 |
| 5.3.3 | UC3: Secure and Trustworthy Mobile Sensing Platform | 78 |
| 5.3.4 | UC4: Secure affective participatory sensing of city events | 80 |
| 5.3.5 | UC5: Smart City Data Marketplace with Secure Multi-Layer Technologies | 83 |
| 5.4 | Exploitation within ongoing and further R&D Projects and Educational Activities | 84 |
| 5.5 | Open Source Approach..... | 85 |
| 5.6 | Sustainability of the M-sec Framework components..... | 85 |



| | | |
|-------|--|-----|
| 5.6.1 | Development and (Security) Designing Tools..... | 86 |
| 5.6.2 | IoT Marketplace FG | 89 |
| 5.6.3 | Devices Security FG & Cloud Tools | 91 |
| 5.6.4 | Privacy Management FG..... | 96 |
| 5.6.5 | Secure City Data Access..... | 98 |
| 5.6.6 | Secured & Trusted Storage FG..... | 100 |
| 5.6.7 | End-to-End Security FG..... | 106 |
| 5.7 | Communication Tools..... | 108 |
| 5.7.1 | Website..... | 108 |
| 5.7.2 | Consortium internal communication and collaboration | 108 |
| 5.8 | Contacts and Resources | 109 |
| 5.8.1 | Contacts..... | 109 |
| 5.8.2 | Resources..... | 109 |
| 6. | Marketing Strategy | 112 |
| 6.1 | Awareness phase..... | 112 |
| 6.2 | Evaluation phase | 112 |
| 6.3 | Conversion and delight phase | 113 |
| 6.4 | Relation with business model canvas..... | 114 |
| 6.5 | Potential activities to be conducted after project ending..... | 114 |
| 7. | Conclusions | 116 |





List of Tables

| | |
|---|-----|
| Table 1. M-Sec Exploitable Security Assets | 15 |
| Table 2. M-Sec Exploitable Security Assets integrated at UC Level | 17 |
| Table 3. M-Sec Exploitable Applications & Devices Assets | 18 |
| Table 4. M-Sec Requirements and Security Threats Coverage | 19 |
| Table 5. M-Sec Key Solution Components..... | 20 |
| Table 6. Summary M-Sec vs Competitive Solutions | 28 |
| Table 7. Value proposition mapping per stakeholder group | 43 |
| Table 8. Summary of partners' exploitation actions | 46 |
| Table 9. SAT & DMSS Sustainability..... | 87 |
| Table 10. MTSA Sustainability | 88 |
| Table 11. IoT Marketplace Sustainability | 90 |
| Table 12. Secured Components for Devices Sustainability | 92 |
| Table 13. Intrusion Detection System Sustainability..... | 92 |
| Table 14. Monitoring & Visualisation Tool Sustainability..... | 93 |
| Table 15. Stealth Security Sustainability | 94 |
| Table 16. GANonymizer Sustainability | 97 |
| Table 17. Eclipse Sensinact Studio & Platform Sustainability | 99 |
| Table 18. Secure SOXfire Sustainability..... | 100 |
| Table 19. Crypto Companion DB Sustainability..... | 101 |
| Table 20. Quorum Blockchain / Blockchain Middleware Sustainability..... | 103 |
| Table 21. T&R Model Engine/Tool Sustainability | 104 |
| Table 22. Security Management Tool Sustainability | 107 |
| Table 23. M-Sec Components Repository | 110 |





List of Figures

| | |
|--|----|
| Figure 1. Relation of T5.2 to other Tasks..... | 13 |
| Figure 2. M-Sec Security Framework by FG..... | 14 |
| Figure 3. M-Sec Security Framework by Layer | 15 |
| Figure 4. M-Sec Use Cases..... | 16 |
| Figure 5. The M-Sec MVP and its possible connections with external systems..... | 22 |
| Figure 6. M-Sec vs BigClouT architecture | 23 |
| Figure 7. Most Common IoT Security Breaches (Source: IoT Analytics Press Research) | 26 |
| Figure 8. Main competitors per layer and company size | 27 |
| Figure 9. Smart City Customer Profile Canvas..... | 34 |
| Figure 10. Smart City Product Canvas | 34 |
| Figure 11. Smart City Main M-Sec Value Proposition & Benefits..... | 35 |
| Figure 12. Developer Community Customer Profile Canvas | 35 |
| Figure 13. Developer Community Product Canvas..... | 36 |
| Figure 14. Developer Community Main M-Sec Value Proposition & Benefits..... | 36 |
| Figure 15. Citizens Customer Profile Canvas | 37 |
| Figure 16. Citizens Community Product Canvas | 37 |
| Figure 17. Citizens Main M-Sec Value Proposition & Benefits..... | 38 |
| Figure 18. IoT Technology Providers Customer Profile Canvas..... | 38 |
| Figure 19. IoT Technology Providers Product Canvas | 39 |
| Figure 20. IoT Technology Providers Main M-Sec Value Proposition & Benefits..... | 39 |
| Figure 21. Research Institutes & Universities Customer Profile Canvas | 40 |
| Figure 22. Research Institutes and Universities Product Canvas | 40 |
| Figure 23. Research Institutes & Universities Main M-Sec Value Proposition & Benefits..... | 41 |
| Figure 24. M-Sec Business Model Canvas | 44 |
| Figure 25. Exploitation & Sustainability Path | 45 |
| Figure 26. Willingness to participate in promotional activities..... | 70 |
| Figure 27. Promotional Activities | 71 |
| Figure 28. Jointly Collaboration..... | 71 |
| Figure 29. Willing to sign a MOU? | 72 |





| | |
|--|-----|
| Figure 30. Willing to sign a third party agreement?..... | 72 |
| Figure 31. The Park Guide web application (Las Llamas Park – UC1)..... | 74 |
| Figure 32. Brochure UC1..... | 74 |
| Figure 33. Value Proposition Use Case 1 | 74 |
| Figure 34. Business Model Canvas Use Case 1 | 75 |
| Figure 35. The Senior Care Web Application (UC2)..... | 76 |
| Figure 36. Brochure UC2..... | 77 |
| Figure 37. Value Proposition UC2..... | 77 |
| Figure 38. Business Model Canvas UC2..... | 78 |
| Figure 39. KEIO Mobile Sensing Platform (UC3)..... | 78 |
| Figure 40. Brochure UC3..... | 79 |
| Figure 41. Value Proposition Canvas UC3 | 79 |
| Figure 42. Business Model Canvas UC3 | 80 |
| Figure 43. Smile City Report App (UC4)..... | 81 |
| Figure 44. Brochure UC4..... | 81 |
| Figure 45. Value Proposition Canvas UC4 | 82 |
| Figure 46. Business Model Canvas UC4..... | 82 |
| Figure 47. Marketplace Front-end (UC5)..... | 83 |
| Figure 48. Brochure UC5..... | 83 |
| Figure 49. Value Proposition Canvas UC5 | 84 |
| Figure 50. Business Model Canvas UC5..... | 84 |
| Figure 51. Development & Security Designing Tools FG Brochure | 86 |
| Figure 52. IoT MarketPlace FG Brochure..... | 89 |
| Figure 53. Device Security FG Brochure | 91 |
| Figure 54. Privacy Management FG Brochure..... | 96 |
| Figure 55. Secure City Data Access FG Brochure..... | 98 |
| Figure 56. Secured & Trusted Storage FG Brochure..... | 101 |
| Figure 57. End to End Security FG Brochure..... | 106 |
| Figure 58. The M-Sec Website..... | 108 |





Glossary

| Acronym | Description | Acronym | Description |
|---------|--|---------|--|
| 5G | 5 th generation mobile communication | M.Sc | Master of Science |
| AI | Artificial Intelligence | MTSA | Modal Transition System Analyzer |
| APPI | Amended Privacy Protection Information | NII | National Institute of Informatics |
| AYTOSAN | Ayuntamiento de Santantander | NTTDMC | Nippon Telegraph and Telephone Data Institute of Management Consultant |
| Bn | Billions | NTTE | Nippon Telegraph and Telephone East |
| CAGR | Compound Annual Growth Rate | NTUA | National Technical University of Athens |
| CCDB | Crypto Companion Database | OS | Open Source |
| CEA | French Alternative Energies and Atomic Energy Commission | P2P | Peer to Peer |
| CRM | Customer Relationship Management | Ph.D. | Doctor of Philosophy |
| CTG | CELESTIA Technologies Group | PII | Personal Identifiable Information |
| D | Deliverable | R&D | Research and Development |
| DPO | Data Protection Officer | SAT | Security Analysis Tool |
| ECE | Electrical and Computer Engineering | SCR | Smile City Report |
| ETSI | European Telecommunications Standards Institute | SDG | Sustainable Development Goals |
| EU | Europe | SESD | Sensor and Electronic Systems department |
| FG | Functional Group | SMEs | Small Medium Enterprises |
| GDPR | General Data Protection Regulation | SW | Software |
| | | T&R | Trust and Reputation |
| ICCS | Institute of Communications and Computer Systems | TPM | Trusted Platform Module |
| | | TRL | Technology Readiness Levels |
| ICN | Information Centric Network | UART | Universal Asynchronous Receiver/Transmitter |
| ICT | Information and Communications Technology | UC | Use Case |
| IoT | Internet of Things | WLI | Worldline |





| | | | |
|-----|------------------------------|-----|------------------------------|
| IPR | Intellectual property rights | WP | Work Package |
| JP | Japan | WU | Waseda University |
| M | Month (of the project) | YNU | Yokohama National University |





1. Introduction and scope

1.1 Introduction

M-Sec has developed a multi-layer secure IoT framework that is compatible with the transfer and processing of personal data between the EU and Japan. The M-Sec framework provides the technological foundation to comply with GDPR, APPI, and the Adequacy Agreement between EU&JP, and it has been validated through five different Use Cases (UCs), among which, two are “cross-border” UCs (i.e. UCs that apply to both EU and Japan).

The goal of this deliverable is to provide a more detailed view of the market possibilities, the M-Sec offering and the business models for a solution like M-Sec. The aim is to provide the final business and exploitation plan to ensure sustainability after the project ends.

In particular, Section 2 presents an overview of the M-Sec Secure framework developed during the length of the project and its key solution components/ modules based on the exploitable assets. Furthermore, it verifies which exploitable assets can be grouped into MVPs with high exploitation potential, based on the requirements and security threats coverage. The same Section also includes the main differences between the M-Sec Project and the BigClouT Project ([BigClouT - Big data meeting Cloud and IoT for empowering the citizen clout in smart cities - EC funded project](#)), highlighting M-Sec enriched some components developed within the frame of the BigClouT Project with security features.

Section 3 provides updates beyond the input provided in the previous version of the document submitted in M24 (“D5.7 Market Analysis and Exploitation activities”). Focusing on the IoT security domain, it focuses on updates of the corresponding market size and the latest competitive landscape.

Section 4 presents the main M-Sec target-stakeholders and the Value Proposition provided by M-Sec for each one of them.

Section 5 describes the strategy for the sustainability and exploitation of M-Sec outcomes. It identifies how each M-Sec core-system component will be specifically maintained - including the current status a list of and future maintenance plans. The Section also focuses on practical sustainability issues, such as the provision of contacts and resources to external interested parties. It also provides the partners’ final exploitation plans, M-Sec joint exploitation strategy, and UC’s driven exploitation.

Section 6 includes the Marketing strategy followed during the length of the project but also future activities to be considered once the project ends.

Finally, the document concludes with a summary of the main topics covered and the key conclusions to take away from this deliverable.

1.2 Relation to other WPs and Tasks

“Task 5.2 - Exploitation activities” receives input from WP2 and in particular from Tasks “Task 2.1 - Use cases description”, “Task 2.2 - Pilots: definition, setup and citizens involvement” through the corresponding deliverables (D2.2, D2.3 & D2.4) and “Task 2.4- Overall system validation and Evaluation” that includes the qualitative and quantitative evaluation of the system.





At the same time, “Task 5.1 - Dissemination and communication activities” and “Task 5.4 - Community building and sustainability activities” are in close alignment to this deliverable, in the sense that both constitute the foundations of creating awareness of project results and succeeding in the exploitation activities.

Furthermore, “Task 3.2 - M-Sec Architecture” and the whole “WP4 - Multi Layered Security” contribute to the identification of components generated before and through the project, the value provided by M-Sec, as well as IPR-related issues. “Task 3.1 - System level and User level Requirements analysis” and “Task 3.3 Risks and security elements for a hyper-connected smart city” contribute to the creation of the Minimum Viable Product of M-Sec based on the requirements and security threats coverage.

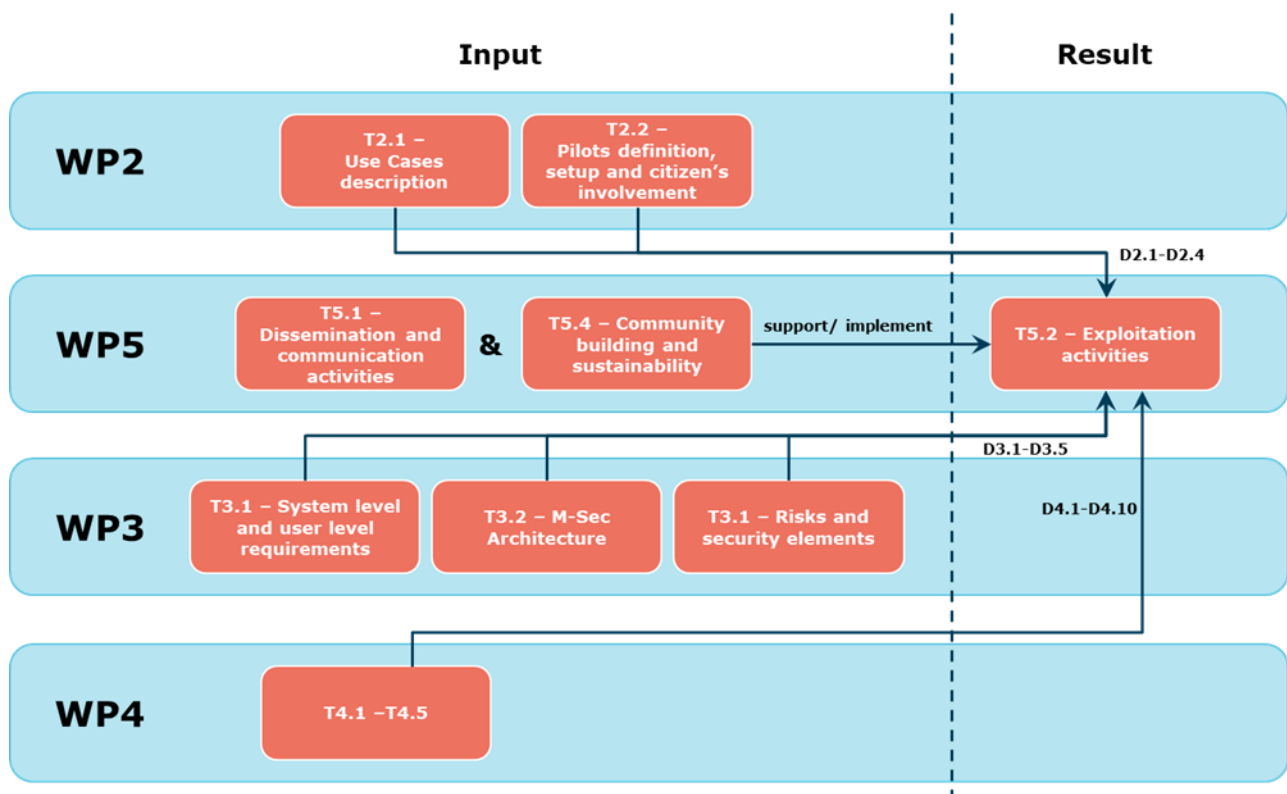


Figure 1. Relation of T5.2 to other Tasks



2. M-Sec Overview

2.1 What is M-Sec

M-Sec was born in July 2018, as an EU&JP R&D Project undertaken by twelve partners (six European and six Japanese). The main motivational factor behind the creation of the project is that many data sources in the IoT and Smart City domain may contain sensitive information, something that raises issues on privacy and data protection. The main objective sought by M-Sec is to develop a framework that provides end-to-end security and integrity of data traffic, from the device to the Cloud and to the application, in a transparent way.

In order to develop a secure end-to-end framework, the consortium based all the developments in identifying and analysing the state of the art of different technologies (IoT, Cloud, Big Data, Blockchain, etc.) and techniques, methods, and mechanisms to reduce vulnerabilities. Risks and threats on current IoT Smart City solutions were also considered for the development of the M-Sec framework.

As a result, the M-Sec framework introduces tools for designing and validating secure applications and providing device-level security that protects IoT devices from malware through intrusion detection mechanisms and vulnerability detection systems, including a secure element to handle the integrity of the device during the boot process and the authentication and encryption for external communication channels. It also entails data security where sensitive data are encrypted and linked to a hash. Thanks to the M-Sec Blockchain and Middleware, the coupling between on-chain and off-chain data and access control becomes possible. Finally, M-Sec expands this security support through end-to-end mechanisms, including authentication and authorisation capabilities.

In order to validate the technical results of the project, the consortium has conducted several pilots ranging from those that collect environmental data (related to noise and temperature levels, air quality) to those that collect infrastructure-monitoring data (garbage disposal amount, unimpaired road marks, etc.) or human-activity data (identifying occupancy levels, monitoring ageing people, etc.).

The two following figures show the end-to-end security value added by M-Sec through the different layers.

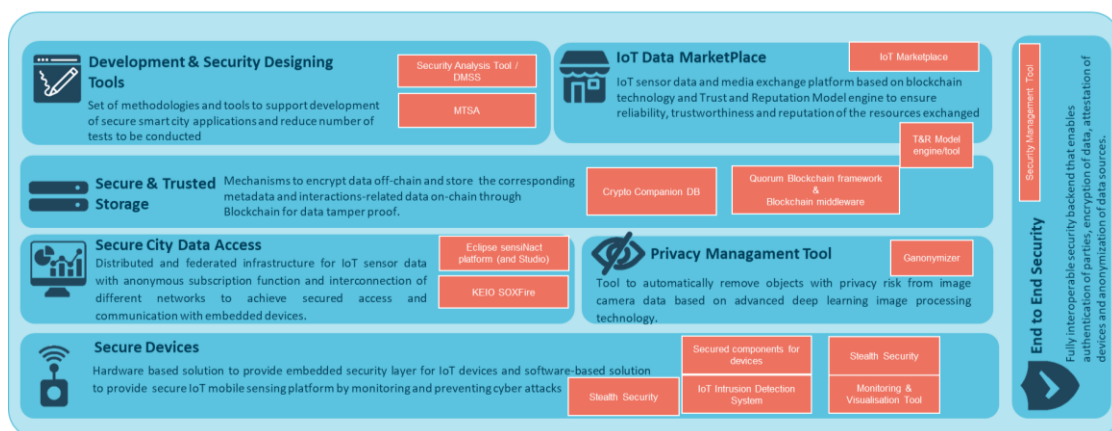


Figure 2. M-Sec Security Framework by FG

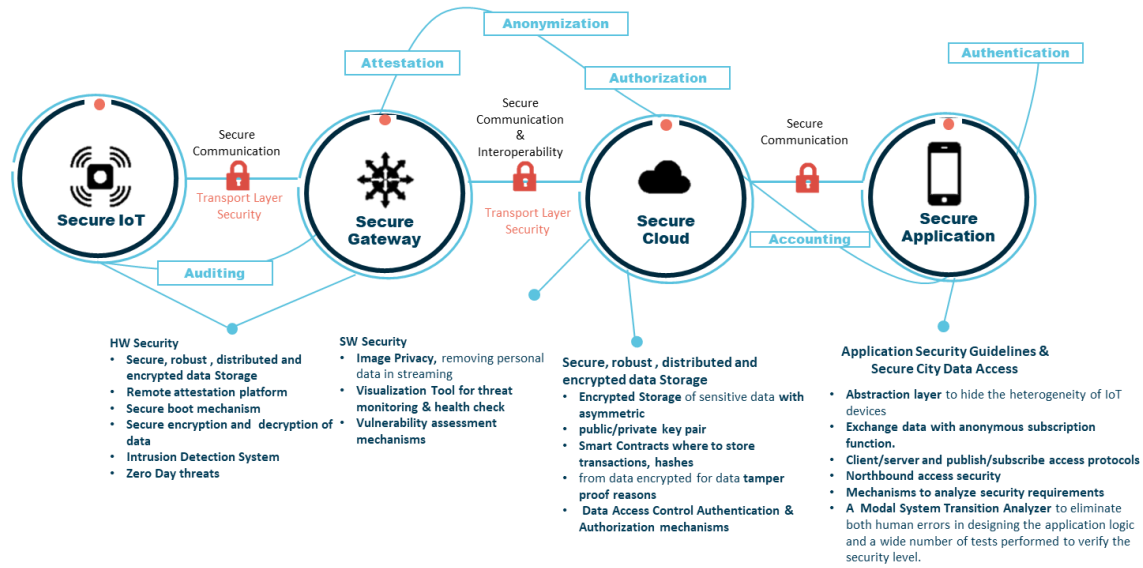


Figure 3. M-Sec Security Framework by Layer

To develop the functionalities of the M-Sec offering, a series of SW components have been developed and/or enhanced within the project, which represent the M-Sec exploitable assets. For more information about the SW components, please refer to deliverables from WP4 submitted in M33. Here, we present the final list of 14 exploitable assets and updated information on OS license, TRL, ownership.

Table 1. M-Sec Exploitable Security Assets

| FG | Component | Owner | Can be exploited individually? | TRL | License |
|--|--|-------|--------------------------------|-----|---|
| Development and (Security) Designing Tools | Security Analysis Tool & Development Method for a Secure Service | NII | No | 4 | Apache License v2.0 |
| | Modal Transition System Analyzer | WU | Yes | 7 | FOSS (no license associated) |
| Cloud Tools FG | Monitoring and Visualization Tool | YNU | No | 6 | Elastic/Apache License |
| Devices Security FG | Stealth Security | YNU | No | 5 | MIT License |
| | Secured Component for Devices | CEA | Yes | 6 | GPL v2.0 (bootloader), Proprietary (OS) |
| | Intrusion Detection System | YNU | No | 7 | OISF/GPL v2.0 license |
| Privacy Management FG | GANonymizer | KEIO | No | 7 | GPL/Proprietary |





| | | | | | |
|------------------------------|--|------|-----|---|----------------------------|
| Secure City Data Access | Eclipse Sensinact Studio& Platform | CEA | Yes | 7 | Eclipse license |
| | Secure SoxFire | KEIO | Yes | 6 | Apache License v2.0 |
| Secured & Trusted Storage FG | Quorum Blockchain /Blockchain Middleware | ICCS | Yes | 7 | Apache License v2.0 |
| | Crypto Companion Database | WLI | Yes | 7 | MIT License |
| | T&R Model Engine/Tool | ICCS | No | 6 | Apache License v2.0 |
| IoT Marketplace FG | IoT MarketPlace | ICCS | Yes | 9 | Apache License v2.0 |
| End-to-End Security FG | Security Management Tool | CEA | Yes | 5 | Mixed Open Source licenses |

In addition to the SW components developed within M-Sec project, five smart city use cases have been implemented through the project lifetime, which represents exploitable assets in themselves. Next, we present the M-Sec exploitable use cases.

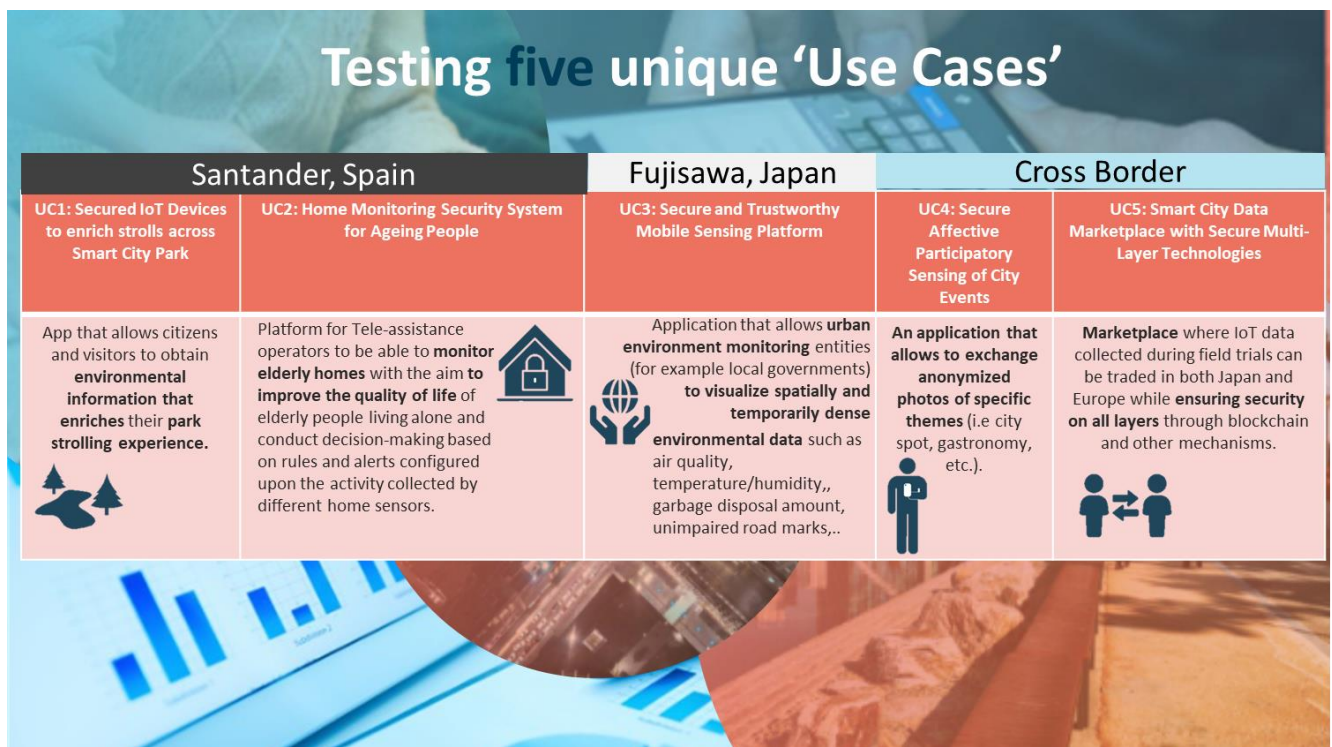


Figure 4. M-Sec Use Cases



The M-Sec Use Cases use different security components provided by M-Sec, as it can be seen below.

Table 2. M-Sec Exploitable Security Assets integrated at UC Level

| FG | Component | UC1 | UC2 | UC3 | UC4 | UC5 |
|--|--|-----|-----|-----|-----|-----|
| Development and (Security) Designing Tools | Security Analysis Tool & Development Method for a Secure Service | | | | ✓ | |
| | Modal Transition System Analyzer | | | ✓ | | |
| Cloud Tools FG | Monitoring and Visualization Tool | | | ✓ | | |
| Devices FG | Stealth Security | | | ✓ | | |
| | Secured Component for Devices | ✓ | | | | |
| | Intrusion Detection System | | | ✓ | | |
| Privacy Management FG | Ganonymizer | | | ✓ | ✓ | |
| Secure City Data Access | Eclipse Sensinact Studio& Platform | ✓ | ✓ | | ✓ | ✓ |
| | Secure SoxFire | | | ✓ | ✓ | ✓ |
| Secured & Trusted Storage FG | Quorum Blockchain /Blockchain Middleware | ✓ | ✓ | ✓ | ✓ | ✓ |
| | Crypto Companion Database | ✓ | ✓ | | | |
| | T&R Model Engine/Tool | | | | | ✓ |
| IoT Marketplace FG | IoT MarketPlace | ✓ | ✓ | ✓ | ✓ | ✓ |
| End-to-End Security FG | Security Management Tool | ✓ | ✓ | ✓ | | ✓ |

From the fourteen M-Sec available components, UC3 is using nine M-Sec security components, followed by UC1, UC4 and UC5 with six components integrated on each one of them, and finally UC2 with a sum of five components. The M-Sec IoT Marketplace and the Quorum Blockchain/ Blockchain Middleware are the two components to be highlighted as they are common for all five UCs.

Some applications and IoT devices are used for the purpose of testing the M-Sec Framework and its core-system components per se and showcasing the M-Sec exploitable results on top of specific “external” systems (of devices, computational entities such as servers, etc.). In other words, these entities are assets that exploit the aforementioned components (Table 2), are not core-system components, but can still be reused from





other projects, even outside the context of M-Sec. Below, we provide an overview of these different extra assets used per use case.

Table 3. M-Sec Exploitable Applications & Devices Assets

| UC | Component | Owner | TRL | License |
|----|--|-------|-----|-----------------|
| 1 | Environmental & Crowded Counter Devices | TST | 7 | Proprietary |
| | Park Guide App | TST | 7 | GPL |
| 2 | Connected Care & Server | WLI | 7 | Proprietary |
| | Caburn Home Monitoring Devices | WLI | 7 | Proprietary |
| 3 | Secure Mobile Sensing Platform | KEIO | 6 | Proprietary |
| | Deep Counter (Garbage Identification AI) | KEIO | 6 | GPL/Proprietary |
| 4 | Smile City Report App & Server | KEIO | 8 | GPL/Proprietary |

2.2 M-Sec Key Solutions Components

During the first two years, an extensive analysis of Requirements and Security Threats took place, in order to identify the main functionalities which have to be delivered by the project in the form of functional components, tools, and mechanisms. The results of the analysis were documented extensively in “D3.2: M-Sec Requirements Analysis” and “D3.5: Risks and security elements for a hyper-connected smart city”. During year 3, work on Requirements and Security Threats continued in the form of fulfilment monitoring (“coverage” of the requirements and security threats from specific results of the project). The final spreadsheets used to document and monitor the requirements and threats are presented as annexes in “D2.8: M-Sec validation and overall evaluation”.

The following two tables provide an overall view of the requirements and security threats from the perspective of functionalities offers (components) of the project. The reported “coverage” can be identified from the aforementioned spreadsheets through the “Related/Affected Asset” and “Covered by (Asset)” columns. In other words, both indirect and direct coverage are taken under consideration in the following metrics of the tables. It should also be noted that the allocation is quantitative and not qualitative. Covering more types of security attacks for example does not imply that the component is more crucial than others. As such, a more in-depth study of the reported results of Task 3.3 and WP4 should take place by those interested in getting a more accurate view.

Finally, it is worth mentioning that the following two tables essentially link specific requirements to security threats, thus linking the results of the Tasks 3.1 with those of Task 3.3.





Table 4. M-Sec Requirements and Security Threats Coverage

| FG | Component | Requirements (% Coverage) | Security Threats (% Coverage) | Relevant Stakeholders |
|--|---|------------------------------|----------------------------------|---|
| Development and (Security) Designing Tools | Security Analysis Tool & Development Method for a Secure Service | 2% | 7% | IoT architects, Integrators, OS Community, NII |
| | Modal Transition System Analyzer | 3% | 7% | IoT architects, Integrators, OS Community, WU |
| Cloud Tools FG | Monitoring and Visualization Tool | 3% | 1% | IoT infra-providers, Service providers, OS Community, YNU |
| Devices FG | Stealth Security | 0% | 1% | IoT infra-providers, Service providers, YNU |
| | Secured Component for Devices | 2% | 3% | IoT infra-providers, Smart Cities, CEA |
| | Intrusion Detection System | 3% | 2% | IoT infra-providers, Service providers, OS Community, YNU |
| Privacy Management FG | GANonymizer | 2% | 1% | Smart Cities, End Users, KEIO |
| Secure City Data Access | Eclipse Sensinact Studio & Platform | 10% | 5% | Service providers, Integrators, Smart Cities, CEA |
| | Secure SoxFire | 10% | 20% | Service providers, Integrators, Smart Cities, KEIO |
| Secured & Trusted Storage FG | Quorum Blockchain / Blockchain Middleware | 6% | 5% | IoT infra-providers, Integrators, Smart Cities, OS Community, ICCS |
| | Crypto Companion Database | 9% | 12% | Service providers, Integrators, Smart Cities, WLI |





| | | | | |
|------------------------|--------------------------|----|-----|--|
| | T&R Model Engine/Tool | 1% | <1% | Service providers, End Users, OS Community, ICCS |
| IoT Marketplace FG | IoT Marketplace | 4% | 10% | IoT infra-providers, Service providers, Integrators, Smart Cities, End Users, OS Community, ICCS |
| End-to-End Security FG | Security Management Tool | 7% | 10% | Service providers, Integrators, CEA |

Table 5. M-Sec Key Solution Components

| FG | Component | Main Requirements covered | Security Threats Covered |
|--|--|--|--|
| Development and (Security) Designing Tools | Security Analysis Tool & Development Method for a Secure Service | Security design capabilities for internal use within the project, during the design phase | Extreme cases identified, which could probably be missed without use of tools (e.g., Thr.App.01, Thr.App.07, Thr.App.15) |
| | Modal Transition System Analyzer | System environment modelled in a labelled transition system, based on discrete events (e.g., R1.3-5.11-1 to R1.3-5.11-5) | Extreme cases identified, which could probably be missed without use of tools (e.g., Thr.App.01, Thr.App.07, Thr.App.15) |
| Cloud Tools FG | Monitoring and Visualization Tool | Monitoring mechanism to continuously collect and report activity metrics, anomaly detection, attacks (e.g., R1.1-4.10-1, R2.1-6.18-6, R2.1-6.2-2, R2.1-6.18-2) | Monitoring mechanism to continuously collect and report activity metrics, anomaly detection, attacks |
| Devices FG | Stealth Security | Zero-day or unknown attacks | Zero-day or unknown attacks |
| | Secured Component for Devices | Providing protection of existing devices systems through HW (e.g. R2.3-6.2-1) | An unauthorized party can read/modify data or configuration parameters on the device (e.g., Thr.IoT.01-Thr.IoT.04) |
| | Intrusion Detection System | Detection of attacks on the devices level (e.g., R2.1-6.2-1) | Detection of attacks on the devices level |

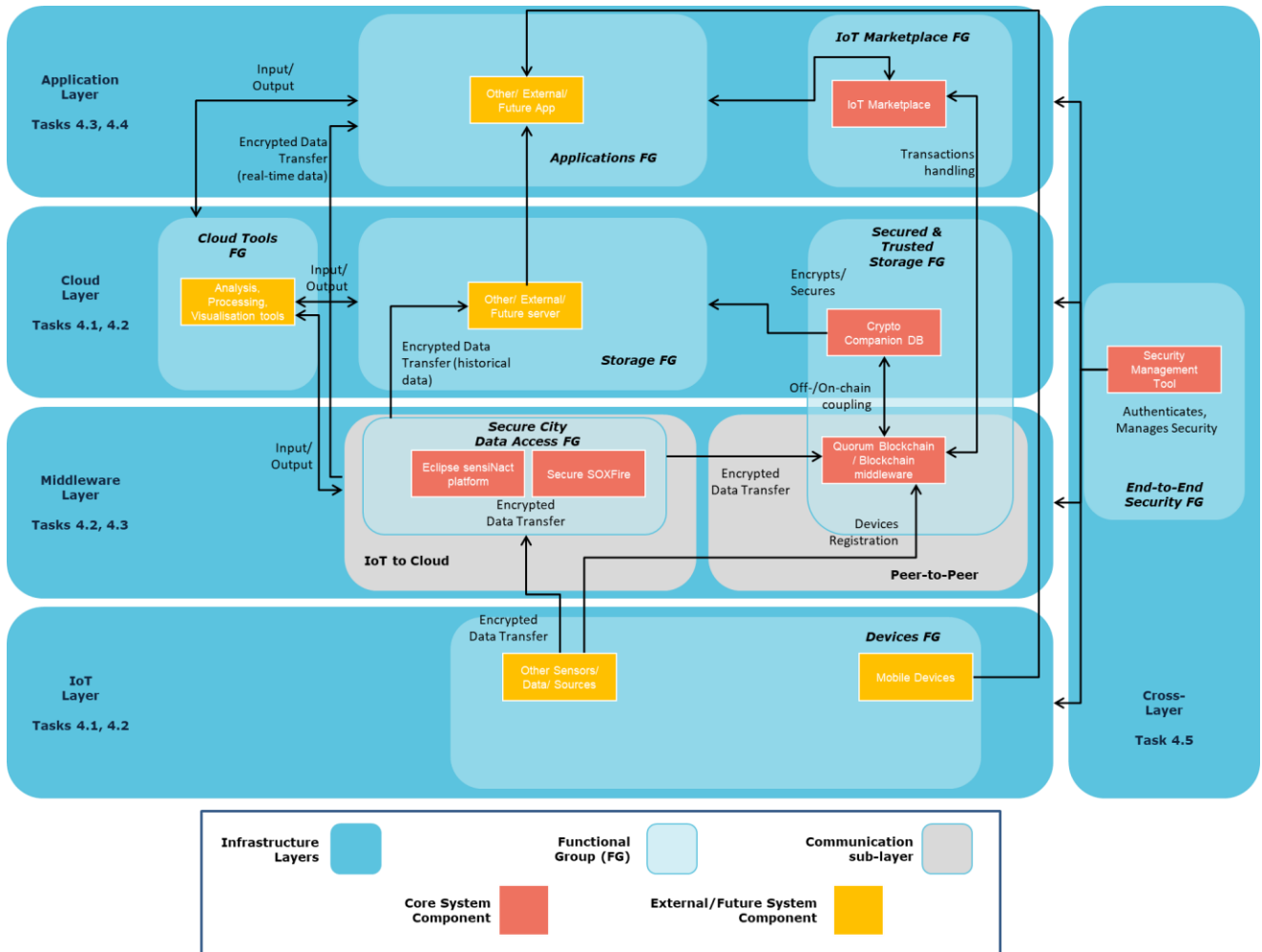




| | | | |
|------------------------------|---|---|--|
| Privacy Management FG | GANonymizer | Automated image anonymization for privacy protection (e.g., R2.2-6.17-8, R2.3-6.17-3) | Automated image anonymization for privacy protection |
| Secure City Data Access | Eclipse Sensinact Studio & Platform | Data and data streams from heterogeneous data sources (IoT devices, online data, etc.) and link o applications (e.g., R2.2-6.6-1 to R2.1-6.6-4) | Integrated with the Security Management Tool to face authorization/authentication threats. |
| | Secure SoxFire | Data (streams) from heterogeneous sources (IoT devices, online data, etc.) accessed through secure link to avoid tampering, leaking, hacking (e.g., R2.2-6.2-3, R1.1-1.1-1, R1.1-3.6-1 to R1.1-3.6-5) | Communications related threats, from the data source to the intermediate storage target (e.g., Thr.Com.01) |
| Secured & Trusted Storage FG | Quorum Blockchain / Blockchain Middleware | Smart contract support for automatic transactions execute (e.g., R1.3-3.8-1) | Malicious agents may make fake transactions (Thr.App.21) |
| | Crypto Companion Database | Secure storage of collected private data (R2.1-6.5-1, R2.1-6.5-3, R2.2-6.5-1, R2.3-6.5-1, R2.3-6.17-2) | Stored Data may be compromised (e.g., Thr.App.2- Thr.App.05, Thr.App.09, Thr.App.12, Thr.App.14) |
| | T&R Model Engine/Tool | Mechanism for content validation (e.g., R1.1-3.5-3, R2.1-6.5-2) | Malicious agents may upload fake data (Thr.App.22) |
| IoT Marketplace FG | IoT Marketplace | Environment for users to share and exchange data (e.g., R1.1-3.8-1) | Integrated with the Quorum Blockchain / Blockchain Middleware, facing related attacks |
| End-to-End Security FG | Security Management Tool | Authentication, authorization, and roles/ passwords management in applications (e.g., R2.1-6.7-9 to R2.1-6.7-13). | Communications eavesdrop, unrestricted access, lack of authentication (e.g., Thr.Com.01 to Thr.Com.04). |

At this point, it is possible to identify the Minimum Viable Product (MVP) that M-Sec can offer, by focusing on components with high TRL (Table 1), covering a large number of requirements and security threats (Table 4 & Table 5), and that can be used and have been tested in a wide range of Use Cases (Table 2).





2.3 Main differences between M-Sec Project and BigClouT Project

As the consortia of M-Sec and BigClouT consisted of some common partners (CEA, NITTEast, NII, ICCS, etc.), some results and ideas that originated from BigClouT were naturally transferred to M-Sec. However, as the two projects have a different focus (BigClouT for applications development vs M-Sec for security in Smart Cities), from a functional point of view, they share only a few points of contact, as it is shown in Figure 6.

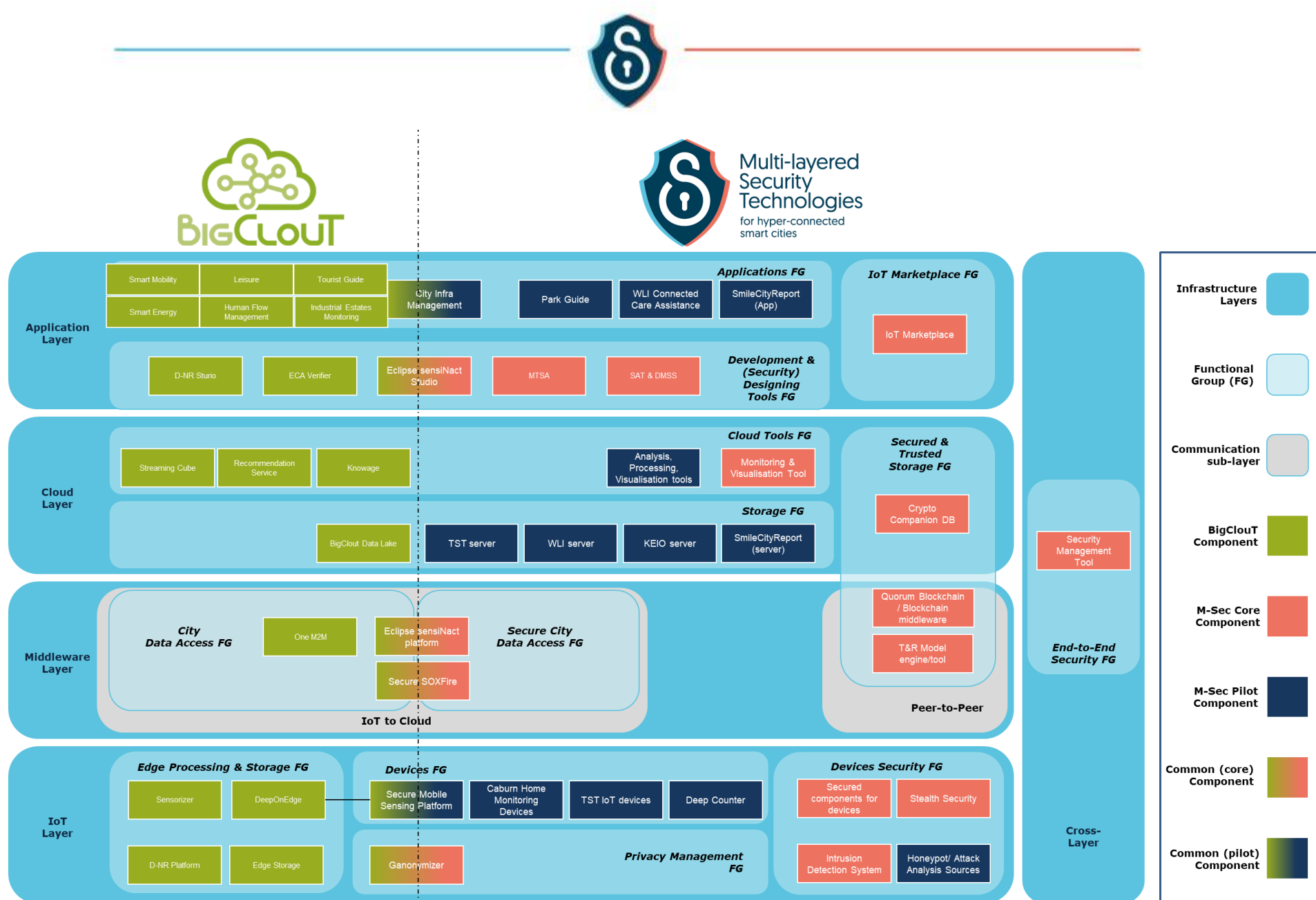


Figure 6. M-Sec vs BigCloudT architecture



Regarding the IoT Layer, BigClouT offers edge processing and storage capabilities (Edge Processing & Storage FG) through several tools, something that is out of the scope of M-Sec. In its turn, M-Sec offers Security tools on the devices level (Devices Security FG). BigClouT mainly focused on already existing, online available datasets, whereas M-Sec used devices as pilot (non-core) components (Devices FG) that were deployed under the context of the project in three UCs (UC1-UC3), as well as mobile devices (UC4). Overall, in this layer, the two projects share two common components: the Mobile Sensing Platform and Ganonymizer. During the M-Sec lifecycle, Mobile Sensing Platform was upgraded (on the communication and the HW side) so as to enhance its security, while Ganonymizer got a new version with more reliable results.

Regarding the Middleware Layer, both projects exploited two main components so as to achieve access to city data sources: sensiNact and SOXFire. The latter was enhanced in order to evolve the component to **Secure** SOXFire (e.g., through the use of appropriate protocols/ encryption). Both components can be supported by the Security Management Tool provided by M-Sec. M-Sec went beyond the traditional “IoT-to-Cloud” flow of data and extended its development activities on the “Peer-to-Peer” level. As a result, the M-Sec blockchain was introduced.

On the Cloud Layer, there is absolutely no connection between the two projects. Regarding the Storage FG, BigClouT introduced a Data Lake of its own for the aggregation of all the data used in the several UCs of the project. On the other hand, M-Sec used different servers depending on the UC, and, in place of a common Data Lake, it introduced a common IoT Marketplace. A marketplace of that sort not only makes it easier to exploit, disseminate, and, in some cases, monetize the produced data, but it also makes the centralized aggregation of datasets unnecessary. Furthermore, on the matter of storage, M-Sec introduced several security elements, such as the Crypto Companion DB (encrypting the data when stored), coupled with the M-Sec blockchain functionalities, thus offering extra security and ensuring tamper-proof record of transactions and interactions. On the other hand, BigClouT offered a variety of Analysis and Visualization tools, while M-Sec only used as pilot components some tools for the analysis and visualization of data per Use Case, and a “Monitoring & Visualization Tool” coupled with the IDS component of M-Sec to monitor network activity and security threats of the system.

On the Application Layer, both projects introduced their own Application tools, with sensiNact Studio being used by both of them for the implementation of some of the pilots. While BigClouT focused on Development tools though, M-Sec used Security Designing tools during its design phase. Regarding the applications/UCs introduced by the projects per se, the only common scenario is that of the “City Infrastructure Management” (M-Sec UC3), where cameras are used on garbage tracks to identify road surface conditions. At the same level, the M-Sec IoT Marketplace brings together all the data produced by other UCs and unifies them under a common data sharing scenario.

Finally, unlike BigClouT, M-Sec includes mechanisms that have a cross-layer applicability. The Security Management Tool offers authentication, authorization, password management, etc. capabilities that, linked to the rest of the M-Sec components, provide end-to-end security.





3. Updates on the Market Size & Competitive Landscape

3.1 Market Overview

The popularity of the Internet of Things (IoT) trend continues to see explosive growth. According to Statista², there are about 21.5 billion interconnected devices in the world. The global IoT security market size is expected to grow from USD 12.5 billion in 2020 to USD 36.6 billion by 2025, at a CAGR of 23.9%. Key factors driving the growth of this market are rising security concerns for critical infrastructure, increasing ransomware attacks on IoT devices, increasing data risk in IoT networks, and growing IoT security regulations³.

The emergence of the smart city concept is the driving force for the rise in demand for IoT Security. As the population is growing, the need for sustainable development and innovative solutions that can cover today's societal challenges is larger than ever before. Smart cities have to be equipped with tools for handling high traffic, population control, and better security for people. A prerequisite to face effectively such tasks is the installation of IoT Devices in the smart cities. This involves connecting devices to one another and enabling them to exchange data in a secure manner, to form clusters, and then to provide a final solution⁴.

However, increasing number of reported breaches and the fear of losing data are among some factors limiting the market growth. It has also been noticed that many users have no insight into how their data are being protected by the cloud vendors.

On the other side, COVID-19 has disrupted normal life and has enforced a substantial change in the policies, priorities and activities of individuals, organizations, and governments. Covid-19 has resulted in the increase of IoT exposures. Remote work and remote schooling have spiked our reliance on IoT systems to a scale no one could have predicted. IoT risks have been a medium-priority, but now, Covid-19 has pushed IoT exposures to the front line.

In September 2020, IBM X-Force reported that IoT attacks observed from October 2019 through June 2020 rose by 400% compared to the combined number of IoT attacks in the previous two years⁵.

² [Global IoT and non-IoT connections 2010-2025 | Statista](#)

³ [IoT Security Market Size, Share and Global Market Forecast to 2025 | MarketsandMarkets](#)

⁴ [Global IoT Security Market Data And Industry Growth Analysis \(thebusinessresearchcompany.com\)](#)

⁵ [IBM X-Force discovers Mozi botnet accounts for 90% of IoT traffic \(iottechnews.com\)](#)





According to the IoT Analytics Press Research⁶, the most common IoT breaches that happened between 2015-2017 were caused by malware (24%), followed by “man in the middle” (22%), brute force (18%) and denial of service (15%) attacks.

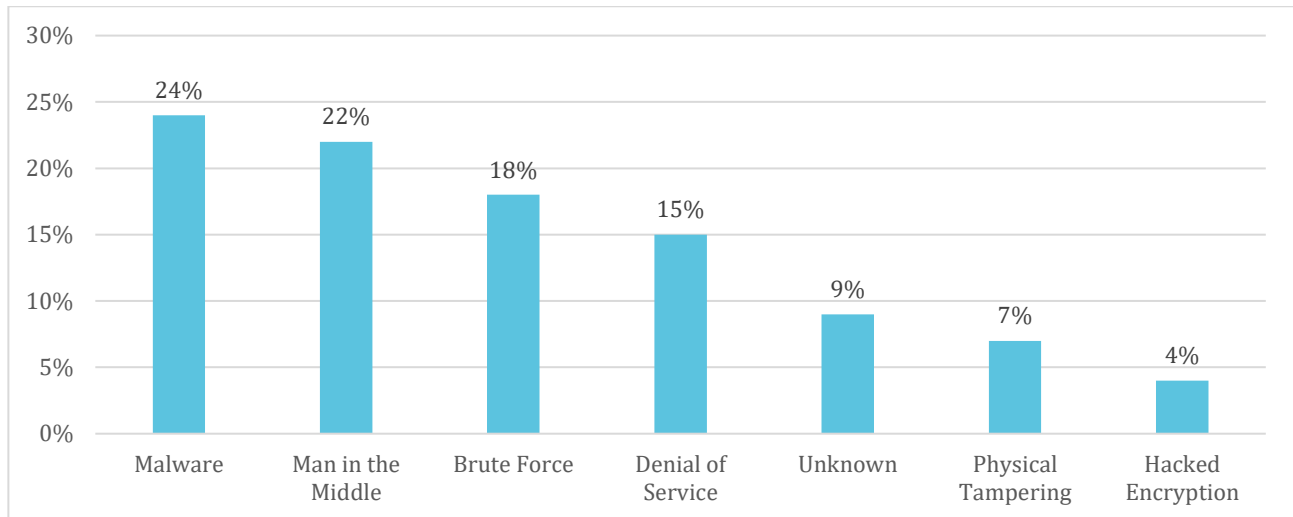


Figure 7. Most Common IoT Security Breaches (Source: IoT Analytics Press Research)

Governments across the globe are focusing on implementing stringent regulations regarding data security and privacy. Various regulations have been introduced to strengthen the security of IoT devices and avoid misuse of data. Such a regulations are GDPR or ETSI TS 103 645⁷, a globally first applicable standard for consumer IoT security standard introduced by the European Telecommunications Standards Institute (ETSI), so as to keep a security baseline for all internet-connected consumer products and provide a basis for future IoT certification schemes.

In addition, new emerging technologies such as blockchain, Artificial intelligence, Machine Learning, etc. will facilitate the developments of new solutions focused on end-to-end protection of IoT Applications. For instance, blockchain is able to monitor the data collected by the sensors ensuring that the whole process is tamper-proof (or at least, in case of tampering, the tampering is detected quickly). Sensors can also transfer data using Blockchain technology, without the need for a trusted third party. Other technologies such as Machine learning can be used to discover vulnerabilities in a system. While this can be useful for those trying to secure a system to intelligently search for vulnerabilities that need to be patched, attackers also use this technology to locate and exploit vulnerabilities in their target system⁸.

3.2 Competitive Landscape

To conduct the competitors' analysis, on the previous version of this deliverable (“D5.7 Market Analysis and Exploitation”) submitted in year 2 of the project, the consortium listed the major competitors per different segment of IoT Platforms. The segments are as follows:

- **Cloud Centric:** IoT Platform with strengths specialising in cloud functions

⁶ <https://iiot-world.com/reports/an-overview-of-the-iiot-security-market-report-2017-2022/>

⁷ https://www.etsi.org/deliver/etsi_ts/103600_103699/103645/01.01.01_60/ts_103645v010101p.pdf

⁸ [Role of Artificial Intelligence in the Internet of Things \(IoT\) cybersecurity | SpringerLink](#)





- **Industry Centric:** IoT Platform with strengths specialising in a specific industry
- **Communications and Device Centric:** Product categories with strengths specialising in communication carriers and devices
- **SME Platform:** Small and medium-sized IoT Platform category that is not as large as large companies
- **Open Source:** Free (including Freemium) Platform category.

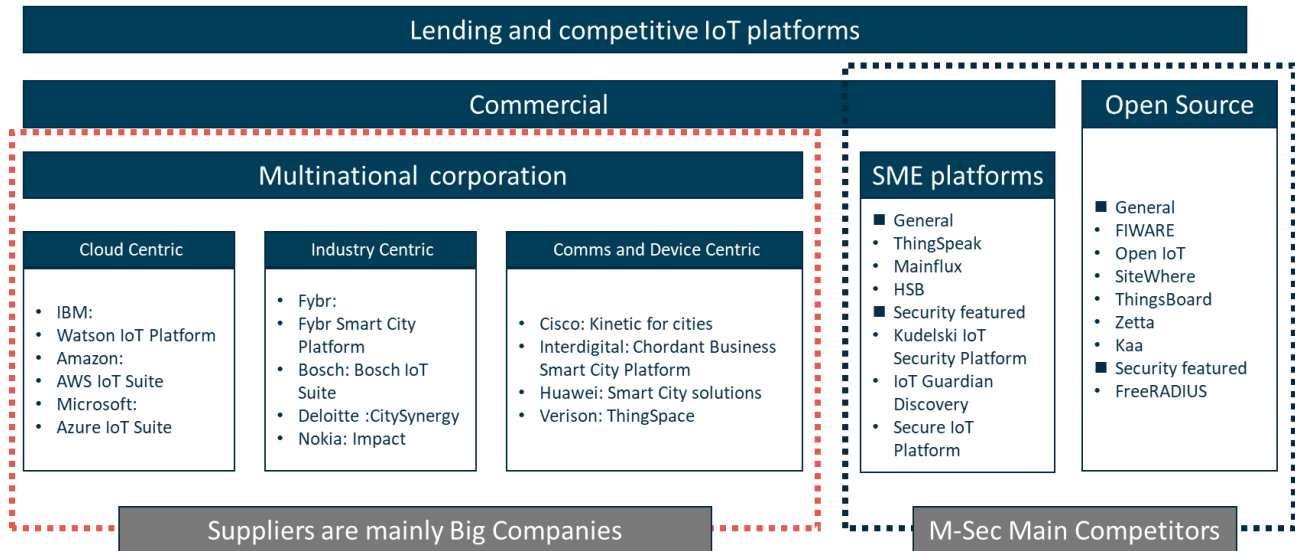


Figure 8. Main competitors per layer and company size

For the competitors' analysis, the consortium has decided to focus on SMEs and open-source software segments that are particularly competitive compared to the characteristics of the M-Sec project, and from these segments, competitive products are investigated. Among the above segments, we are investigating the products that are characterised by the security functions that are the main features provided by M-Sec project. The following table summarises this comparison between M-Sec and the above competitors.





Table 6. Summary M-Sec vs Competitive Solutions

| Competitor | Description | Target User | Distribution Channel | Business Model | Pricing | Strengths | Weaknesses |
|--------------------------------|---|---|--|--|-------------|---|--|
| M-Sec | End-to-end secure platform covering all layers of the IoT ecosystem with security enhancement and data integrity and protection mechanisms. | Japanese and EU IoT vendors, organizations and municipalities | Web, partner's channels and potential clients, .. | License fee from using the platform + optional services based on demand. | Freemium | <ul style="list-style-type: none">A low-cost, flexible and scalable IoT paradigm based on an open-reference architecture, adequate for hyper-connected smart citiesValidation in real-life UC in Santander and Fujisawa, recognised for their long-term "smart city" approach. | <ul style="list-style-type: none">Insufficient way to earn moneyPromotional and Marketing is not sufficient compared to competitors.There is no association with hardware Partners or vendors regarding distribution channels. |
| Secure IoT Platform | <p>Promotes security standardisation initiatives that include everything, from the manufacturing stage of IoT devices to services in the cloud environment.</p> <p>The secure IoT platform enables safe and secure management of IoT devices throughout their life cycle, from manufacturing to installation / operation and disposal.</p> | Japanese ICT system vendors and device makers | Web and distribution with Hardware Partners | Membership | Unavailable | <ul style="list-style-type: none">IoT security standards that can be used for Japanese IoT marketParticipation of some major security vendors | <ul style="list-style-type: none">Activities are based on research not actual business.Focused only in Japan. |
| IoT Guardian Discovery | <p>AI-powered, cloud-based platform that detects, identifies, secures, and provides insights into IoT devices. Guardian sensors send data to Vantage for consolidated security management anywhere, anytime from the cloud.</p> <p>They can also send data to the Central Management Console for aggregated data analysis at the edge or in the public cloud.</p> | Network managers and smart-city infrastructure management sectors | Partnering with global major ICT companies, such as Cisco and VMWare | License fee from using the platform + on demand optional services | Unavailable | <ul style="list-style-type: none">AI based securityMajor partnersSecurity Operation Center support security managementDashboard has good usabilityReal time situational awareness | <ul style="list-style-type: none">Smart city is just one of its uses, therefore it has not unique smart-city-based characteristics. |
| Kudelski IoT Security Platform | Protect against IoT threats & create new business opportunities. | IoT system and service providers | Unclarified | License fee from using the platform | Unavailable | <ul style="list-style-type: none">Partnership with major public cloud providersDevice managementInvolvement in IoT devices design | <ul style="list-style-type: none">Smart city is just one of its uses, therefore it has not unique smart-city-based characteristics |





IoT security is a set of technologies and best practices to ensure the sustainability of your IoT business: it provides trust, integrity and control. It protects key assets like devices, identity, data, decisions, commands and actions.

- Support client's business model
- Lifecycle support of IoT devices

| | | | | | | | |
|------------|---|---|---|-------------|------|---|---|
| FreeRADIUS | <p>RADIUS, which stands for "Remote Authentication Dial In User Service", is a network protocol - a system that defines rules and conventions for communication between network devices - for remote user authentication and accounting. Commonly used by Internet Service Providers (ISPs), cellular network providers, and corporate and educational networks, the RADIUS protocol serves three primary functions:</p> <ul style="list-style-type: none">· Authenticates users or devices before allowing them access to a network· Authorizes those users or devices for specific network services· Accounts for and tracks the usage of those services. | Used by huge amount of OS SW developers for digital authentication. | Major OS distributors, such as RedHat, are involved in its distribution | Open Source | Free | <ul style="list-style-type: none">• Digital authentication• Long history of its safety• 100 million users | <ul style="list-style-type: none">• Covering just small part of IoT security platform and function. |
|------------|---|---|---|-------------|------|---|---|

Competitor

Product Characteristics

Security Characteristics

| | | |
|-------|---|--|
| M-Sec | <ul style="list-style-type: none">• OPEN TECHNOLOGIES AND ARCHITECTURAL PATTERNS: A low-cost, flexible and scalable IoT paradigm achieved through an open-reference architecture, adequate for hyper-connected smart cities• IoT MARKETPLACE BASED ON BLOCKCHAINS: An IoT devices marketplace where data are exchanged through the use of virtual currencies, for real-time matching of supply and demand. | <ul style="list-style-type: none">• MULTI-LAYER SECURITY SUPPORT: Comprehensive security support ensuring security and privacy across all layers of the systems, from the device level to the network and application level. |
|-------|---|--|





- It is organized by introduction layer (device manufacturing layer/network layer/data management layer/service layer)/industry/device usage
- The Secure IoT Platform (SIOTP) performs multi-step authentication by combining a secure element with embedded identification information that identifies an IoT device and an electronic certificate issued by an international standard electronic certificate authority, from the time of manufacture. It maintains a consistent trust chain of products until disposal to prevent data tampering and spoofing.
- The secure element, which is the root of trust, can utilize the hardware secure element with excellent tamper resistance manufactured by the IC chip vendor linked with SIOTP, and breaks the trust chain even if it is physically attacked. It is possible to operate without being affected

- You can protect a wide variety of mixed environments with rapid asset discovery, network visualization and accelerated security.
- Every Vantage license includes an unlimited number of Guardian virtual sensor licenses, enabling you to deploy Guardian sensors wherever you want to increase your visibility and security.

- Establish Trust: Give every IoT device a unique identity that is immutable, unclonable and forms the foundation for any IoT security function.
- Ensure Integrity: Protect data at rest and in motion, ensuring it is authentic, comes from a verified source and hasn't been tampered with.
- Enforce Control: Prevent unauthorized commands or software from being executed on a device, and control access to data using fine-grained policies.
- Full product lifecycle: Respond to evolving threats and new security requirements by actively managing the product from launch through end of life, using advanced security technology and services

- A RADIUS server is a critical part of a network security system. Any successful attack on a RADIUS server means that anyone can be authenticated, with potentially catastrophic consequences. Two requirements are necessary for any secure server; secure source code, and secure configuration.
- The Source Code is Secure: The security page contains the public record of security issues in FreeRADIUS. (Try asking a commercial vendor for that information!) The source code is freely available, including the complete history of all changes. Our policy is to be transparent and open about all security issues with the server. While this policy may seem to open the server to attacks from





people looking at the source code, the reality is different. That openness has permitted us to be part of the Coverity scan project for many years. All of the issues found by Coverity have been fixed. That is, the code has been scanned for a large class of potential issues, and has been proven to not be vulnerable to those issues.

- "Fail-Safe" Configuration: The server configuration is designed to be "fail-safe". The default configuration requires administrator edits before any user can be authenticated. The default configuration and internal policy is to reject all requests that have not successfully been authenticated.





Through the competitors' analysis process, some of the strengths and weaknesses of the M-Sec positioning are clarified. The main M-Sec strengths are the following parts:

- **Real-life Pilots in Spain and Japan:** Validation in real-life UCs in Santander and Fujisawa, recognized for their long-term “smart city” approach. At M-Sec, multiple UCs have been verified through demonstrations. Of great importance is also the fact that certain UCs also acquire a cross-border as common demonstrations connecting Japan and the EU are provided. In the cross-border UCs between Japan and the EU, the Japanese Personal Information Protection Law and the EU's GDPR are being compared and examined, and the elements that are helpful from a legal point of view are organized. These UCs have been demonstrated based on the competitive characteristics of M-Sec.
- **Open Technologies and Architectural Patterns:** A low-cost, flexible, and scalable IoT paradigm is achieved in M-Sec, through an open-reference architecture, adequate for hyper-connected smart cities. M-Sec allows users to configure low-cost, flexible components. It includes free software and has a wide range of service areas, which makes it possible to approach smart-city issues widely. Among other competing products, there are some that have a low-priced and highly flexible component configuration, but there are few that guarantee security at the same time in a wide range of areas.
- **Multi-Layer Security Support:** M-Sec provides comprehensive security support ensuring security and privacy across all layers of the system, from the devices and network level to the application one. M-Sec incorporates components (e.g. Monitoring & Visualization Tool) that ensure security for each layer, and also introduces a Security Management Tool that ensures end-to-end security for the entire architecture. Each component itself is a concept technology that is also used in other IoT platforms, but the design that comprehensively guarantees security in multiple layers such as applications and IoT layers is new. Some security components are new and distinctive, such as the ability to anonymously process personal information. With this multi-layer security, new users can develop services while ensuring security and reducing interference between each component in an integrated manner.
- **IoT Marketplace based on blockchain:** M-Sec offers an IoT devices marketplace where data are exchanged through the use of virtual currencies, for real-time matching of supply and demand. In the IoT marketplace, data collected from multiple applications and IoT devices can be bought and sold between third parties. The marketplace provides a mechanism that is easy for participants to use, while ensuring the security of data transmission and reception using blockchain technology.

On the other hand, the main M-Sec weaknesses are:

- M-Sec does not have association with hardware partners or vendors regarding distribution channel.
- The way to earn money to sustain the project is not necessarily sufficient.
- The key factor is recognition of the product from many users. Even though it is not the scope of the project, marketing and promotional activities are not sufficient compared to those of competitors. When more and more users start using M-Sec and realise that M-Sec is valuable, the options for M-Sec will increase.





4. M-Sec Value Proposition & Relevant Stakeholders

In this Section, we provide the final version of the building blocks of the M-Sec Value Proposition Canvas per stakeholder, as identified in the previous Market Analysis and Exploitation report (D5.7).

The main M-Sec Stakeholders are the following:

- Smart Cities
- Developers Community
- Citizens
- IoT Technology Providers
- Research Institutes & Universities

For each one of these groups, the consortium provides an analysis of the value proposition canvas. The Value Proposition Canvas is formed around two building blocks – customer profile and a company's value proposition⁹:

- Customer Profile
 - Gains – the benefits which the customer expects and needs, what would delight customers and the things which may increase likelihood of adopting a value proposition.
 - Pains – the negative experiences, emotions and risks that the customer experiences in the process of getting the job done.
 - Customer jobs – the functional, social, and emotional tasks customers are trying to perform, problems they are trying to solve and needs they wish to satisfy.
- Value Map
 - Gain creators – how the product or service creates customer gains and how it offers added value to the customer.
 - Pain relievers – a description of exactly how the product or service alleviates customer pains.
 - Products and services – the products and services that create gain and relieve pain, and which underpin the creation of value for the customer.

4.1 Smart Cities

Municipalities, city councils and city administration, and National and Regional Governments are considered in the analysis. The main challenge for public institutions is to find and deploy easily scalable technologies that bring tangible benefits (better services, reduced costs, covered citizen's needs), but at the same time include reliable and robust security and privacy mechanisms to deal with any potential malicious attacks or breaches on sensitive information.

⁹ <https://www.b2binternational.com/research/methods/faq/what-is-the-value-proposition-canvas/>





4.1.1 Customer Profile

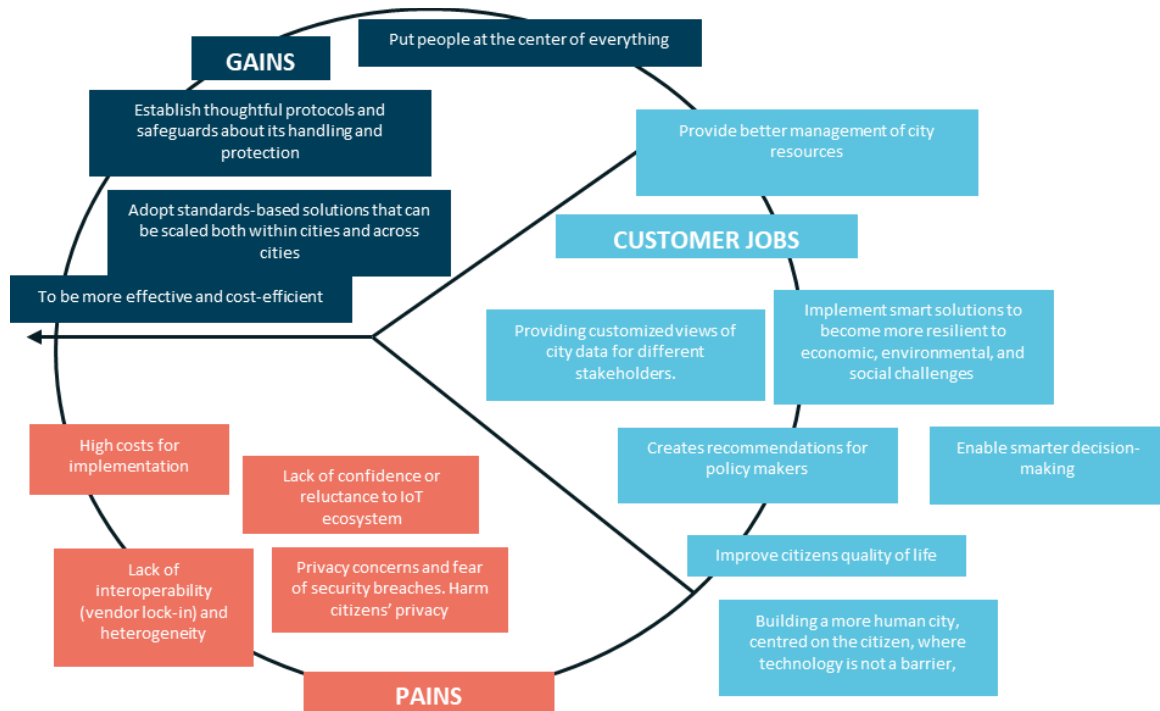


Figure 9. Smart City Customer Profile Canvas

4.1.2 Product

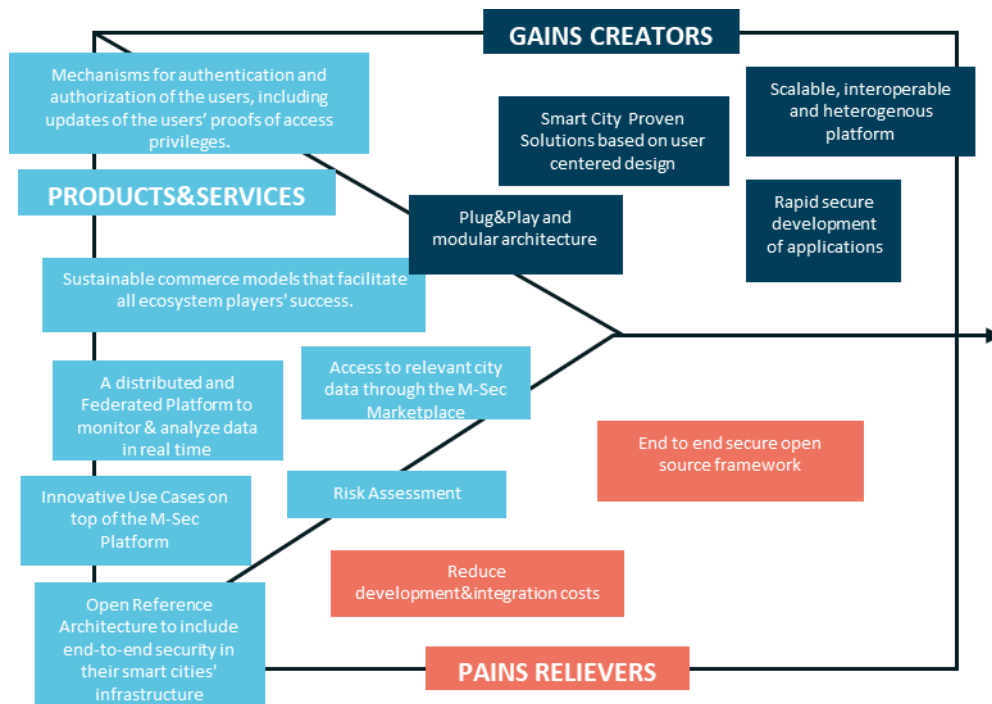


Figure 10. Smart City Product Canvas





4.1.3 Main Value Proposition & Benefits

| | | | | |
|---------------------|--|--|---|--|
| Strategic Objective | M-Sec looks forward to working closely with Government and Smart Cities to enforce Data protection whilst continuing to promote innovation within the IoT Ecosystem | | | |
| Value Proposition | M-Sec provides a low-cost, flexible and open-reference architecture to deploy IoT Smart City Application in an end-to-end approach to address current economic, environmental, and social challenges without compromising user's privacy data and ensuring data reliability and integrity to make and implement strategic decisions in a smart city context. | | | |
| Key Benefits | Risk Assessment study for threat and security threats faced hyper-connected smart cities <i>D3.5 Risks & Security Elements for a hyper-connected smart city</i> Deliverables - M-Sec (mseproject.eu) | Open Source & Flexible Architecture A market-ready open source software, with a modular approach combining components that enhances end to end IoT security on each of the IoT layers (device, cloud, application). M-Sec-H2020(github.com) | Distributed and federated platform in a way that is scalable, extensible, easy to use, allowing interoperability and heterogeneity, thus coexist and benefit from the richness of the variety | Smart City Proven Use Cases Innovative demonstrable Use Cases to address Sustainable challenges, increase of ageing people and isolation, and social interaction. M-Sec Use Cases have been developed based on commerce models that facilitate all ecosystem players' success. Use Cases - M-Sec (mseproject.eu) |
| | User Centered Design based on the collection of end users requirements. <i>D3.2 M-Sec Requirements Analysis</i> Deliverables - M-Sec (mseproject.eu) | | A secure end-to-end tested and validated Framework Includes mechanisms for authentication and authorization of the users, intrusion detection system and vulnerability assessment, automatic personal data deletion in stream, encrypted data at rest and in motion.. | |
| | GDPR & APPI compliance M-Sec provides specific modules to deal with the data rights and access constraints (right for portability, right to be forgotten, ...) | | | |

Figure 11. Smart City Main M-Sec Value Proposition & Benefits

4.2 Developers Community

Independent programmers who are willing to experiment and engage with M-Sec components to build IoT applications on top. The main challenge for developers is the lack of expertise on applying security standards correctly along with the adoption of new regulations (e.g. GDPR).

4.2.1 Customer Profile

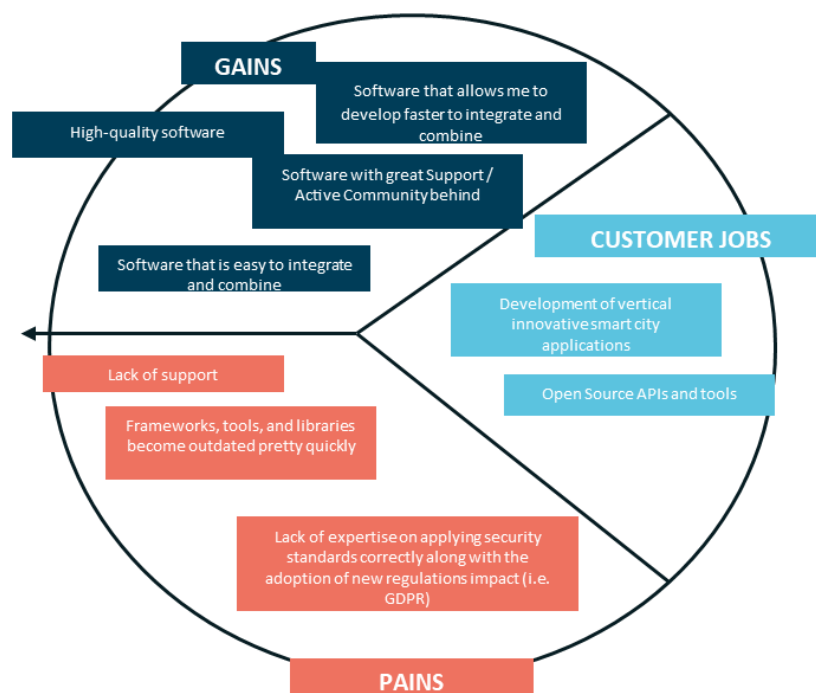


Figure 12. Developer Community Customer Profile Canvas



4.2.2 Product

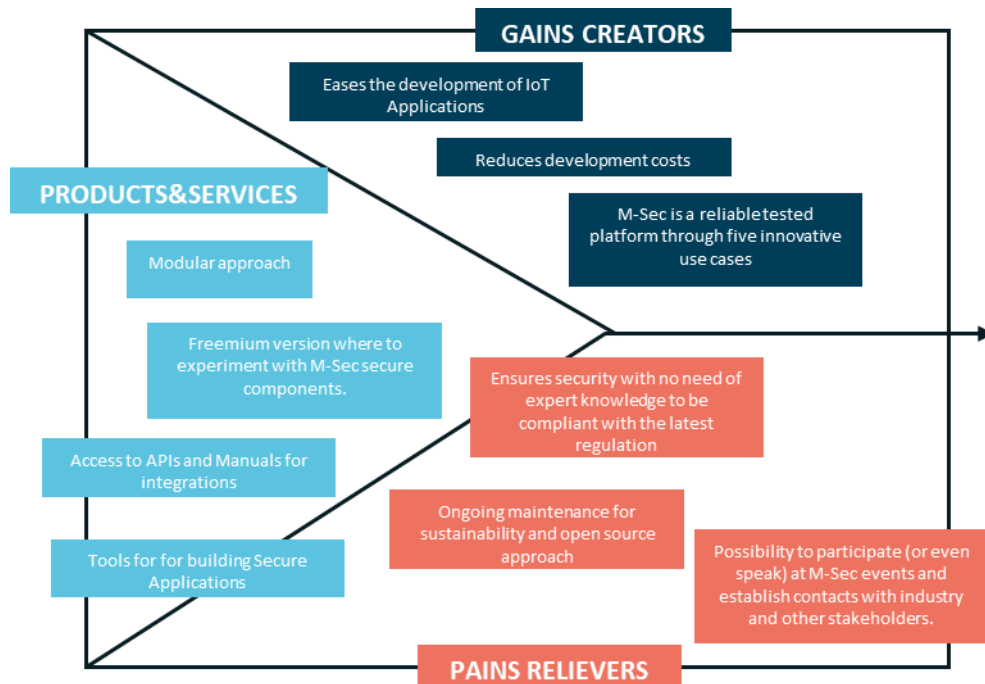


Figure 13. Developer Community Product Canvas

4.2.3 Main Value Proposition & Benefits

| | | | |
|---------------------|---|---|---|
| Strategic Objective | M-Sec eases the development of IoT Applications while reducing development costs and ensuring security with no need of expert knowledge to be compliant with the latest regulations through its secure framework based on end-to-end IoT Layer solution. | | |
| Value Proposition | M-Sec provides an end-to-end secure platform build based on privacy by design and gets your job done with littler effort. It has a modular approach, meaning that it is possible to re-architect as the need changes. It offers a Freemium version where to experiment with M-Sec secure components. The consortiums provides access to open source APIs and Manuals for integrations and installation. | | |
| Key Benefits | Open Source & Flexible Architecture A market-ready open source software, with a modular approach combining components that enhances end to end IoT security on each of the IoT layers (device, cloud, application). MSec-H2020(github.com) | A secure end-to-end tested and validated Framework Includes mechanisms for authentication and authorization of the users, intrusion detection system and vulnerability assessment, automatic personal data deletion in stream, encrypted data at rest and in motion.. | A community with expert partners on several technologies where links among incubators, business networks, universities and developers communities are provided to share IoT challenges and findings. M-Sec Smart City Ecosystem - M-Sec (msecproject.eu) |
| | | Development much faster and compliance with regulations M-Sec enables focusing on what is specific to add security on the smart IoT applications. M-Sec provides specific modules to deal with the data rights and access constraints (right for portability, right to be forgotten, ...) | |
| | | Developer Kit Access to a set of tools , guidelines to develop secure applications and Projects Results | |

Figure 14. Developer Community Main M-Sec Value Proposition & Benefits

4.3 Citizens

The lack of confidence or reluctance to IoT ecosystem, not feeling attracted to available Smart City Use Cases, and awareness about protection of personal data are the main big concerns related to this stakeholder group.



4.3.1 Customer Profile

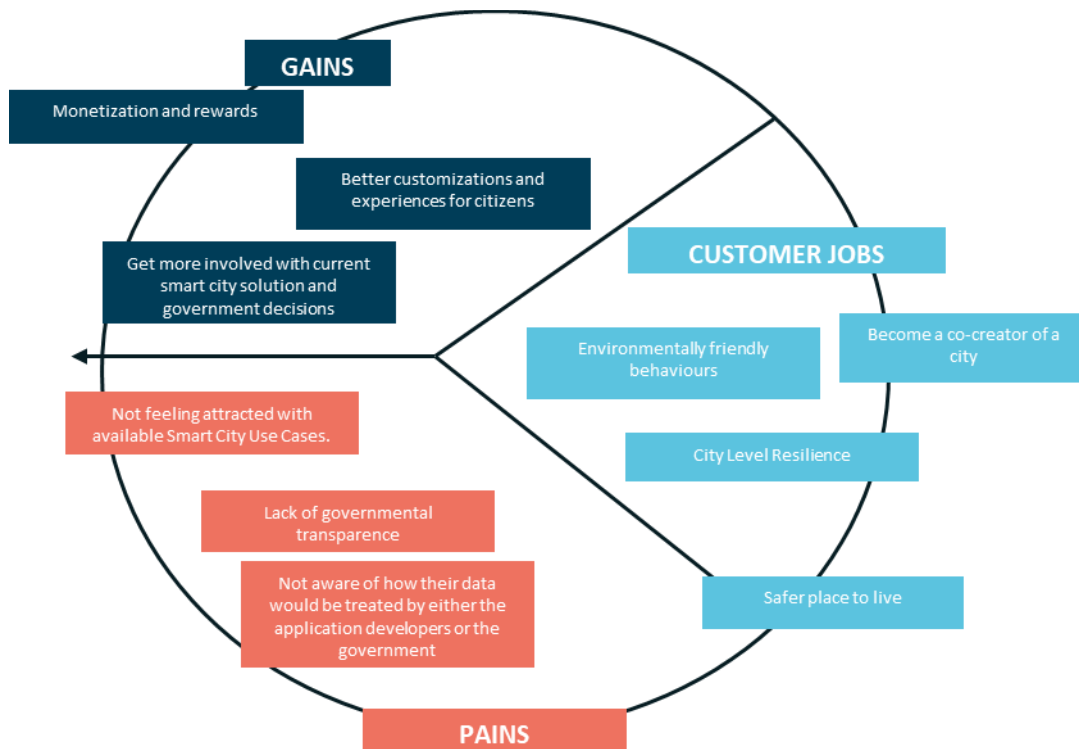


Figure 15. Citizens Customer Profile Canvas

4.3.2 Product

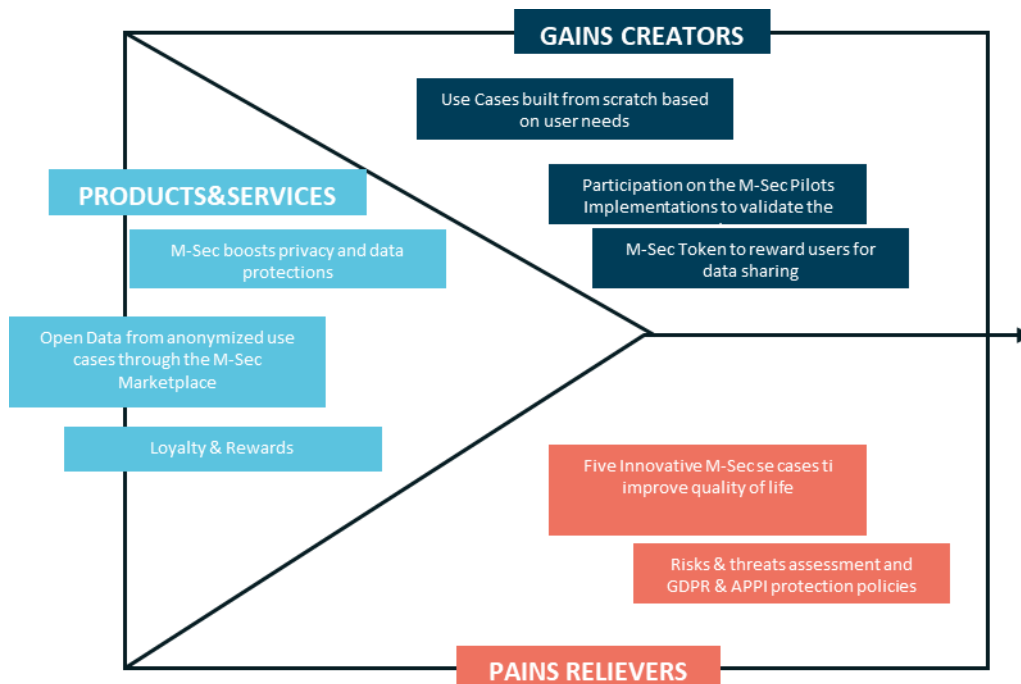


Figure 16. Citizens Community Product Canvas



4.3.3 Main Value Proposition & Benefits

| | | | | |
|---------------------|---|---|---|--|
| Strategic Objective | M-Sec will bring new IoT security standards to ensure end-to-end data privacy by building a reliable and trustworthiness IoT ecosystem. | | | |
| Value Proposition | M-Sec provides five innovative Smart City Use Cases ranging from environmental monitorization to home monitorization for ageing people to sharing pictures from the city for fun. All the applications use cases are based on principles of end to end security to secure the integrity, accountability and privacy of your personal data. Are you curious? | | | |
| Key Benefits | 5 new use cases for smart city oriented applications to improve quality of life through IoT devices Use Cases - M-Sec (mseproject.eu) | An IoT devices marketplace where information and services are exchanged through the use of virtual currencies blocksplace.com | Boost awareness about Privacy Protection Regulations based on GDPR & APPI <i>D5.11 M-Sec GDPR Compliance Assessment Report</i> <i>D3.5 Risks & Security Elements for a hyper-connected smart city</i> Deliverables - M-Sec (mseproject.eu) | Gamification to become part of the Smart City Transformation as Citizen as a sensor by sharing valuable data with the city and other citizens. Leverage in M-Sec Token |

Figure 17. Citizens Main M-Sec Value Proposition & Benefits

4.4 IoT Technology Providers

IoT devices and sensors, services, and applications providers and integrators. The main challenge for this group is the fact that competitive pressure for shorter times to market and cheaper products drive many designers and manufacturers of IoT systems (including devices, services, and applications) to devote less time and resources on security.

4.4.1 Customer Profile

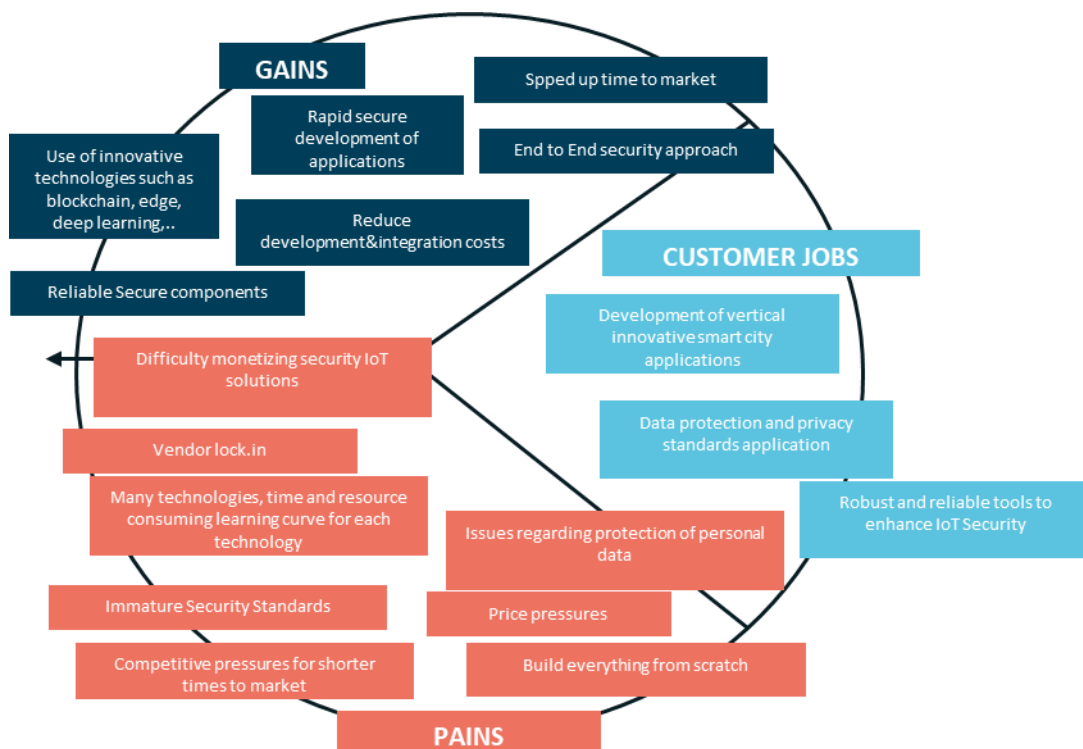


Figure 18. IoT Technology Providers Customer Profile Canvas



4.4.2 Product

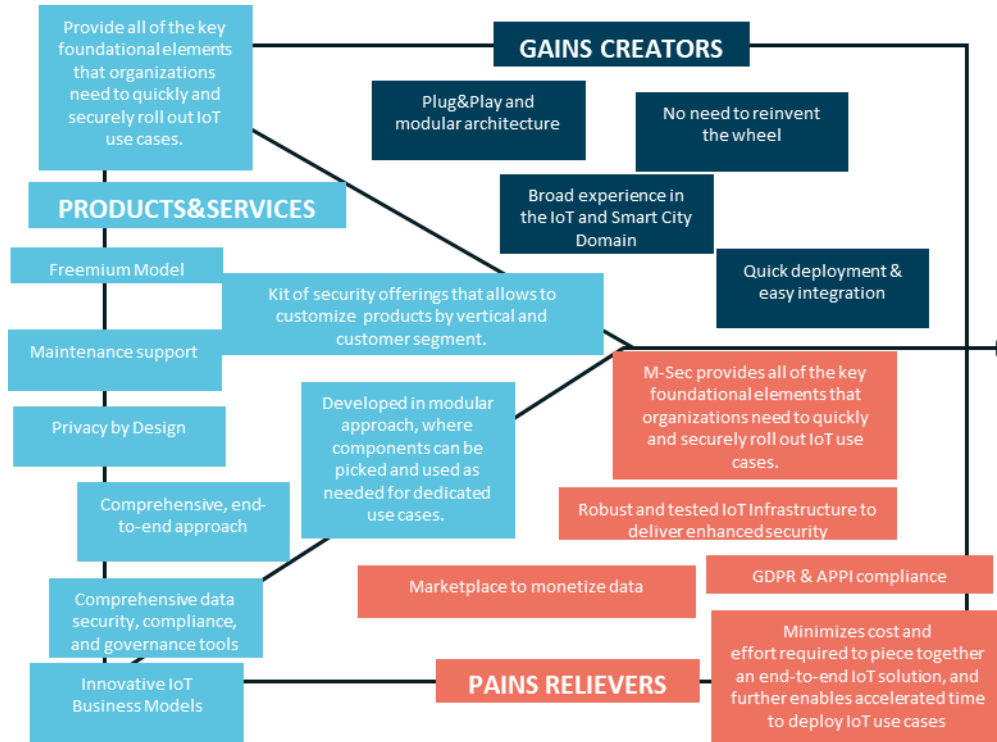


Figure 19. IoT Technology Providers Product Canvas

4.4.3 Main Value Proposition & Benefits

| | | | |
|---------------------|--|---|---|
| Strategic Objective | M-Sec will bring new IoT security standards to ensure end-to-end data privacy by building a reliable and trustworthiness IoT ecosystem. | | |
| Value Proposition | M-Sec provides a developed end to end secure IoT framework where to build innovative smart city applications on top of it while enabling the creation of liquid markets with profitable business models. | | |
| Key Benefits | Open Source & Flexible Architecture A market-ready open source software, with a modular approach combining components that enhances end to end IoT security on each of the IoT layers (device, cloud, application). M-Sec-H2020(github.com) | A secure end-to-end tested and validated Framework Includes mechanisms for authentication and authorization of the users, intrusion detection system and vulnerability assessment, automatic personal data deletion in stream, encrypted data at rest and in motion.. | GDPR & APPI compliance M-Sec provides specific modules to deal with the data rights and access constraints (right for portability, right to be forgotten, ...) |
| | User Centered Design based on the collection of end users requirements. <i>D3.2 M-Sec Requirements Analysis</i> Deliverables - M-Sec (msecproject.eu) | Development much faster and compliance with regulations M-Sec enables focusing on what is specific to add security on the smart IoT applications. M-Sec provides specific modules to deal with the data rights and access constraints (right for portability, right to be forgotten, ...) | Marketplace to exchange anonymized data for business or research analysis blockspalace.com |
| | | | Developer Kit Access to a set of tools , guidelines to develop secure applications and Projects Results |
| | | | Smart City Proven Use Cases Innovative demonstrable Use Cases to address Sustainable challenges, increase of ageing people and isolation, and social interaction. M-Sec Use Cases have been developed based on commerce models that facilitate all ecosystem players' success. Use Cases - M-Sec (msecproject.eu) |

Figure 20. IoT Technology Providers Main M-Sec Value Proposition & Benefits





4.5 Research Institutes & Universities

Technical Universities and Research organisations boosting innovation projects with a practical application. The main challenge for them is to understand the practical applicability of the research results, e.g. connectivity challenges, cloud-based challenges (network delays, throughput, reliability), security mechanisms, etc. as well as the visibility of the main achievements and outcomes.

4.5.1 Customer Profile

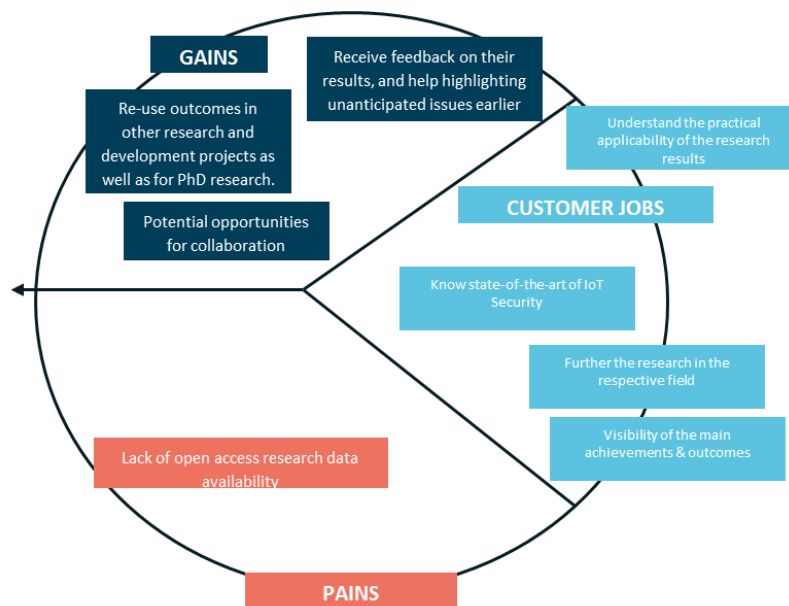


Figure 21. Research Institutes & Universities Customer Profile Canvas

4.5.2 Product

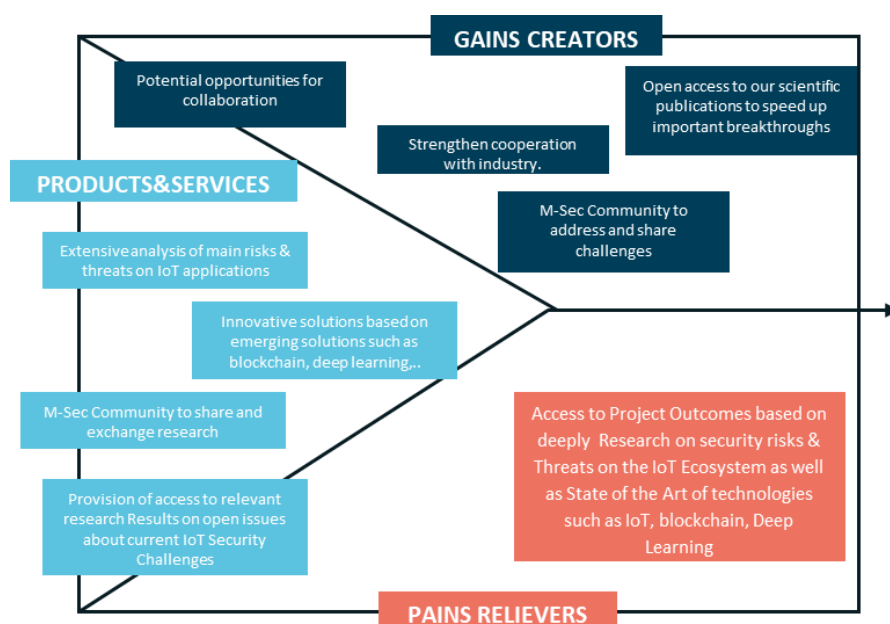


Figure 22. Research Institutes and Universities Product Canvas



4.5.3 Main Value Proposition & Benefits

| | | | | |
|---------------------|---|---|---|--|
| Strategic Objective | Be update with new findings to be at the forefront of research by becoming an active member of the M-Sec community. | | | |
| Value Proposition | M-Sec provides an ecosystem to strengthen cooperation with industry, networking and sharing scientific expertise, potential collaborations). In addition, it provides research outcomes based on current IoT Security Challenges thanks the twelve partners composing the consortium with expertise in different technologies. | | | |
| Key Benefits | A community with expert partners on several technologies where links among incubators, business networks, universities and developers communities are provided to share IoT challenges and findings. M-Sec Smart City Ecosystem - M-Sec (mseccproject.eu) | Risk Assessment study for threat and security threats faced hyper-connected smart cities <i>D3.5 Risks & Security Elements for a hyper-connected smart city</i> Deliverables - M-Sec (mseccproject.eu) | Research on current State of the Art and development of innovative solutions to overcome current IoT Security Challenges WP4 deliverables Deliverables - M-Sec (mseccproject.eu) | Open access to our scientific publications to speed up important breakthroughs Scientific Papers - M-Sec (mseccproject.eu) |

Figure 23. Research Institutes & Universities Main M-Sec Value Proposition & Benefits

4.6 M-Sec overall Value Proposition

Taking into account the value propositions conducted per stakeholder, the consortium presents the final Business Model Canvas of the whole M-Sec (see Figure 24).

Customer Segment

For the customer segment, the identified stakeholders are:

- Smart Cities
 - Municipalities
 - City Councils
 - National and Regional Governments
- Developers Community
- Citizens
- IoT Providers (IoT manufacturers, cloud service providers, applications providers, integrators)
 - Startups & SMEs
 - ICT Companies
- Research Centres & Universities

Channels

Channels used for bringing the value of M-Sec to stakeholders are:

- Consortium Partners' Channels (social networks, company websites, Companies' Product portfolio)
- Third Party Channels (strategic alliances created)
- M-Sec Website and Social networks
- Github for open source code sharing and collaboration



Customer relationship

- Organisation of and participation to global events, workshops, webinars
- Partners Networks and customer base
- M-Sec Community Ecosystem (a community with expert partners on several technologies and business networks, universities, developers groups, etc.).

Key Activities

- Consultation. IoT security expertise to protect IoT Applications from today's security threats. Helping end-users identify, understand, and manage security risks against all aspects of IoT systems.
- Integration. Technical support to integrate M-Sec components with customers' infrastructures.

Key Resources

The key resources are the input that makes it possible to perform the key activities and operate the business model.

- European Funding Programmes
- High Technical Skilled Human Resources

Key Partners

- Pilot Cities
- M-Sec partners
- European Commission & National Institute of Information and Communications Technology
- Smart Cities Strategic Alliance
- Relevant Standardisation Bodies
- Strategic Partnerships per Domain
- Data Providers

Cost Structure

- Product development and maintenance costs
- Personnel costs
- Marketing costs
- Infrastructure costs

Revenue Stream

- Agreements with customers for key projects
- Licensing
- Consulting Services
- Integration Support

Value Proposition

In the following table, the consortium provides the final value proposition of M-Sec, mapping outcomes with stakeholders needs.



Table 7.Value proposition mapping per stakeholder group

| Value Proposition | IoT Tech providers | Smart Cities | Citizens | Developers Communities | Research Institutes/ Universities |
|---|--------------------|--------------|----------|------------------------|-----------------------------------|
| Open Reference Architecture to include end-to-end security in smart cities' infrastructure. | ✓ | ✓ | | ✓ | |
| Smart City Proven Use Cases Innovative demonstrable Use Cases to address Sustainable challenges, increase of ageing people and isolation, and social interaction. M-Sec UCs have been developed based on commerce models that facilitate the success of all ecosystem players. | ✓ | ✓ | ✓ | | |
| Distributed and federated platform in a way that is scalable, extensible, and easy to use, allowing interoperability and heterogeneity, which leads to benefits from the data richness and variety. | | ✓ | | | |
| Access to relevant city data through the M-Sec Marketplace. | ✓ | ✓ | | | ✓ |
| Sustainable commerce models that facilitate all ecosystem players' success. | ✓ | ✓ | | | |
| A tested and validated end-to-end security Framework. Includes mechanisms for authentication and authorization of the users, intrusion detection system and vulnerability assessment, automatic personal data deletion in stream, encrypted data at rest and in motion, etc. | ✓ | ✓ | | ✓ | |
| Risk Assessment study for threat and security threats faced hyper-connected smart cities. | | ✓ | | | ✓ |

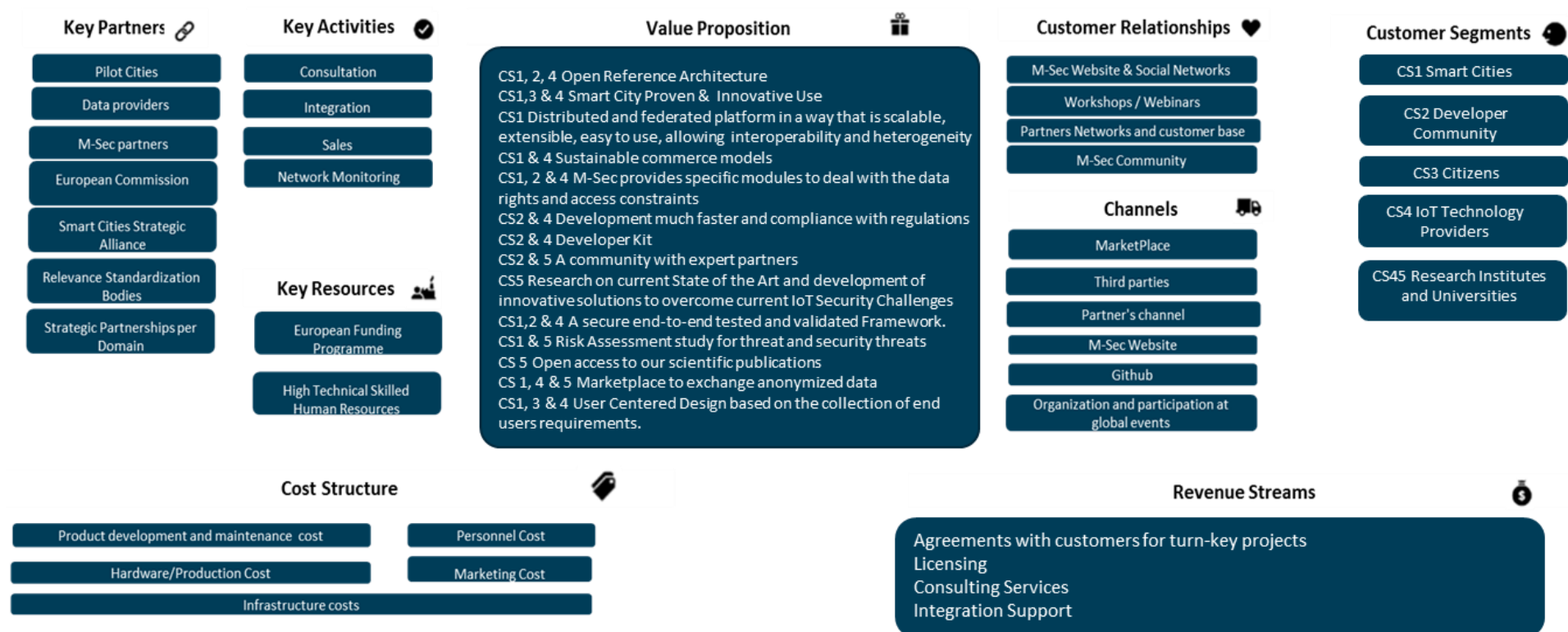


Figure 24. M-Sec Business Model Canvas



5. M-Sec Exploitation and Sustainability Strategy

The M-Sec exploitation and sustainability strategy relies on the next pillars:

- Partners' individual exploitation plans during and after the project.
- Joint Exploitation activities among consortium partners to e.g. jointly develop or exploit further M-Sec assets.
- UC's driven exploitation of some M-Sec Components.
- Synergies with other similar R&D Projects such as Fed4IoT to gain major impact. Use of the SW Components and knowledge gained during the project for ongoing and further R&D and educational activities.
- Open Source approach and upstream contributions to Open Source Communities.
- Sustainability of the exploitable assets developed within M-Sec for at least 12 months after the end of the project.



Figure 25. Exploitation & Sustainability Path













5.1 Partners' Individual Exploitation Plans

M-Sec partners provided an initial version of their exploitation intentions in M12 in D5.6. Here, we present the partners' final exploitation plans once the project is concluded, but also the exploitation achievements accomplished during the project's lifetime.

A summary of the most representative exploitation actions foreseen by partners to exploit M-Sec assets is also presented.



Table 8. Summary of partners' exploitation actions

| Partner | R&D activities & projects | Educational activities | Commercial exploitation | Technology & Knowledge Transfer |
|--|---------------------------|------------------------|-------------------------|---------------------------------|
|  | ✓ | | ✓ | |
|  | ✓ | ✓ | | ✓ |
|  | | ✓ | | ✓ |
|  | ✓ | | ✓ | |
|  | ✓ | | | ✓ |
|  | ✓ | | | |
|  | ✓ | ✓ | ✓ | |
|  | ✓ | ✓ | | |
|  | ✓ | ✓ | | |
|  WASEDA University | | ✓ | | |
|  YOKOHAMA National University | ✓ | ✓ | | |
|  国立情報学研究所 National Institute of Informatics | ✓ | | | |





5.1.1 Worldline

Worldline (<https://worldline.com/en/home.html>) is the biggest European payment-services provider and a leader in digital transformation. With annual revenues of €5.3 Bn and 20,000+ employees worldwide, it specializes in the development of cloud-based platforms that it customizes for its clients and exploits through transactional business models (i.e. pay per use).

Worldline is currently working on existing and future platforms around technologies such as IoT, Artificial Intelligence (AI), Cyber Security, Biometrics, Blockchain, and many others.

Worldline invests very heavily on Research & Development, both via internal projects and via collaborative ones such as the ones included in research programs like H2020. In all of these projects, the objective is always to explore innovation in technologies and business applications that may enhance existing solutions/business lines or create completely new ones. This requirement is also applicable to the M-Sec project. In this sense, Worldline intends to maximize the short and medium term applicability of the developments done under the M-Sec project, so that they can be transferred to the market via future phases of the M-Sec- platform or applied to other projects.

Worldline, apart from being the European Coordinator of M-Sec, also acts as one of the technical partners, contributing to identifying the requirements that must be covered by the M-Sec platform as well as participating in the implementation of the decentralized P2P level security and blockchain and application level security. Worldline, through its Connected Care solution is also the owner of the Home Monitoring Security System for ageing people (UC2).

Focusing on the Worldline individual exploitation plan for M-Sec, the following business objectives are identified:

- To maximize the technical and business expertise around the development of P2P level security and blockchain as well as cloud level security.
- To develop technical assets that could be used in future versions of the project or in other R&D and commercial offers, both by Worldline and by third parties, ensuring in this way the sustainability of the results of the M-Sec project.
- To position itself as the ideal technical and business partner for the M-Sec UC2 in order to develop future phases of the solution or other ones based on security assets. This is also extensible to other third parties who may find Worldline as a good partner for their projects.
- To expand Worldline Business Portfolio with a robust solution as it is Connected Care (UC2), including end-to-end security features provided by M-Sec.

Innovation & exploitation during the project

The innovation and exploitation possibilities explored during the three years of the project are the following:

Year 1:

- During the first year, Worldline explored the current home monitoring tele-assistance solutions that already existed in the market with the aim of providing a solution that ideally covers all the main business aspects and user needs for UC2.
- Meetings with potential suppliers of IoT home monitoring devices took place in order to find a provider who offers affordable devices while providing at the same time high standards on usability and quality.





Caburn Solutions (<https://caburnsolutions.com/>) was the supplier selected to provide the home sensors to be used on UC2. Caburn is an innovative and specialised IoT company with a background in health, environmental, and social-care monitoring.

- A product portfolio based on the evolution of the “Connected Assistance Platform” to the “Connected Care Platform” was created in order to display all the use cases that were applicable for Worldline target customers. In addition, Worldline developed a business model to exploit Connected Care Platform used on UC2 (Home Monitoring Security System for ageing people). The Business Model was based on an operational fee (users/month). Furthermore, the platform could be commercialized as a white label or be customized by adding branding, integrations, new features, and so on.
- The M-Sec project and Connected Care were presented both within the Atos and the Worldline groups as well as to external clients, as a way to express Worldline’s capabilities. Worldline encountered several potential collaboration opportunities around providing security layers on home monitoring. For instance, Worldline conducted several meetings with TiC Salut (public entity that promotes innovation and technology around the health sector). TiC Salut was very interested in identifying how blockchain can be applied on health.
- Worldline agreed with the rest of the consortium partners to run Blockchain on the Alastria Blockchain platform. Alastria is a Quorum-based platform developed by the Alastria consortium, cofounded by Worldline in Spain, which intends to develop a fully legal and scalable multisector Blockchain infrastructure.

Year 2:

- During the second year of the project, Worldline continued evolving the solution Connected Care based on the requirements stated by stakeholders of the M-Sec Project, especially those of Atenzia that is the tele-assistance company testing the solution itself (UC2).
- Product Proposition of Connected Care was defined in a more clear way along with its business model (setup + monthly fee based on the number of devices acquired by the potential client).
- During 2 was marked by the development of the M-Sec framework that would support the provision of the different use cases. The development of the core platform and the different services for each one of the use cases implied the creation of a series of digital assets that could be used to accelerate the development of solutions for third parties.
- Worldline has gained some expertise in aspects such as GDPR and APPI regulations in order to be able to develop, in line to the requirements of data protection and integrity, a secure and safe storage layer that complies with both regulations linked with Blockchain for tamper-proof data.
- Finally, Worldline started presenting the M-Sec project to its existing health and insurance customers, and potential leads for them to participate to the project and/or to explore similar solutions in a more professional manner, thanks to the availability of the initial demonstrators.

Year 3:

- A pilot for UC2 was implemented in order for the M-Sec consortium to receive feedback on what it works and what needs to be mended.
- The pilot has also provided Worldline with much stronger solutions to showcase both M-Sec’s and Worldline’s capabilities to address increasing requirements related with data integrity and security. This has helped Worldline to increase its capacity to convince potential clients.





- Furthermore, the feedback obtained during this period has positioned Worldline as a reference among its peers for the tele-assistance sector, since not many companies have the experience of implementing a real-life project based on a secured framework that provides end-to-end security. Worldline is under discussions with several companies in order to achieve a first client powered to M-Sec assets.
- Finally, Worldline has proposed a collaboration to the UC partners that would like to move to an industrialization phase in their vertical after the conclusion of the M-Sec project.

Innovation & exploitation after project conclusion

Once the project concludes, Worldline intends to work on the following elements to capitalize on the developments achieved during the M-Sec project execution:

- Develop a dissemination and commercial strategy based on the promotion of the results achieved through the pilots validation.
- Explore the use of M-Sec assets in the delivery of existing projects or in commercial proposals. Since M-Sec follows a modular approach this will benefit the viability to re-use the different components developed.
- Collaboration with partners that would like to continue with the technical and commercial development of their vertical solution.
- Increase the commercial push of the Connected Care platform in the health, insurance and Telco sector.
- Open potential collaboration with other consortiums or solutions providers that may complement the value proposition developed by M-Sec.

5.1.2 ICCS

The National Technical University of Athens (NTUA) is the oldest and most prestigious technical university in Greece. It was founded in 1837 and has since been contributing to the progress of the engineering science in Greece, through the education of young engineers and its multi-faceted research and development activities. The School of Electrical and Computer Engineering (ECE) of NTUA is well known in Greece and abroad for the research achievements of its faculty members and the good reputation of its students and alumni. The Institute of Communication and Computer Systems - ICCS (www.iccs.ntua.gr) is a research organisation associated with the ECE school and has about 40 laboratories and research units.

ICCS/NTUA participates in M-Sec through the Distributed, Knowledge and Media Systems Group (DKMS) that focuses on research activities related to advanced distributed computing, dealing with topics such as Service Oriented Architectures, Cloud Computing, Internet of Services and Things, Big Analytics, Security, Blockchains, and Social Networks.

As a research institute which is not for profit, ICCS/NTUA will use the project results for:

- Education, knowledge transfer, consulting, potential software licensing, and the support of entrepreneurship programs for its alumni and students.
- M-Sec is offering ICCS the opportunity to improve competences and skills related to P2P level security and Blockchains: handling new technologies, conducting more in-depth research based on past experiences, applying old and current research outcomes to new domains.
- Through its participation in M-Sec, ICCS aims to develop innovative mechanisms that may be offered to the open source community. Since ICCS/NTUA is a non-profit Academic Research Body, all related results





will be released as open source contributions under Open Source licenses (more specifically, permissive licenses, as they are not restrictive licenses and can be used to create a proprietary good, allowing a commercial exploitation and ensuring high impact).

- Furthermore, ICCS exploits the research projects in which it participates in order to connect them with M.Sc. and Ph.D programme theses as well as the creation of new training courses, for the active engagement of young researchers in a highly innovative environment.

Innovation & exploitation during the project

The innovation and exploitation possibilities explored during the three years of the project are the following:

Year 1:

- During the first year, ICCS explored the current blockchain technologies and IoT integration capabilities for bringing into realization the technology assets that were required by the M-Sec project.
- ICCS agreed with the rest of the consortium partners to run Blockchain on the Alastria Blockchain platform. Alastria is a Quorum-based platform developed by the Alastria consortium, cofounded by Worldline in Spain, which intends to develop a fully legal and scalable multisector Blockchain infrastructure.

Year 2:

- During the second year of the project, ICCS continued evolving the assets that are related to the IoT marketplace and Quorum Blockchain middleware.
- During the specific development, ICCS has created publications and incorporated into its post graduate courses and PhD research programme the specific technologies.
- ICCS started presenting actively the M-Sec project to its collaborators, thanks to the availability of the initial demonstrators.

Year 3:

- A pilot for UC5 was implemented in order for the M-Sec consortium to receive feedback on what it works and what needs to be mended.
- Various webinars and dissemination events took place where the Quorum Blockchain Middleware and IoT Marketplace were presented and demonstrated.
- The basis for the further exploitation and sustainability of the ICCS technology assets has been set during the specific period.
- PhD research activities have been carried out with the help of the specific technology assets.

Innovation & exploitation after project conclusion

The major research outcomes for ICCS in the M-Sec project are: the IoT MarketPlace, the Quorum Blockchain middleware, and the Trust and Reputation Model Engine. The two first assets especially are of vital importance for the operation of the M-Sec UCs. ICCS plans to maintain the specific technology assets not only as part of the M-Sec sustainability beyond its lifecycle, but also as a basis for future research that will lead to their extension.

Once the project concludes, ICCS intends to work on the following elements to capitalize on the developments achieved during the M-Sec project execution:





- Explore the use of M-Sec assets in the delivery of existing projects or future ones. Since M-Sec follows a modular approach this will benefit the viability to re-use the different components developed. To this direction, for example, in the TruBlo H2020 project (<https://www.trublo.eu/>) ICCS is taking advantage of implementations, experience, and technical knowledge from M-Sec components such as the IoT Marketplace. Similarly, in the Pledger H2020 project (<http://www.pledger-project.eu/>), ICCS will build on top of its experience of creating smart contracts (acquired within the context of M-Sec) to create an SLAs-Smart Contracts bridge: a tool to “translate” Service Level Agreements for cloud services into Smart Contracts within blockchains.
- Explore the use of M-Sec assets for further internal research and enhancements of the post-graduate level courses and PhD Program.
- Collaboration with partners that would like to continue with the technical and commercial development of their vertical solution.
- Open potential collaboration with other consortiums or solutions providers that may complement the value proposition developed by M-Sec.

5.1.3 Ayuntamiento Santander

The city of Santander is working in an economic and social transformation, fostering a smart, innovative and open to society city model, with the aim of offering more efficient and better quality urban services through the use of new technologies, and stimulating business opportunities and employment creation. Santander’s vision of a smart city focuses mainly on citizens, where technology is used as a tool to provide more efficient urban services, which will result in an improvement in their quality of life.

Santander City Council takes an active part in European research projects, such as M-Sec, for more than ten years. As a result of the pilots carried out in this type of projects, the city enriches the current urban laboratory through the deployment of new devices, the use of new technologies as well as the development of new services or applications that aim to improve the quality of life of citizens.

In addition, participating in this type of project allows Santander to strengthen its international projection as a Smart City, reinforcing collaborations with consortium partners and attracting not only new opportunities for partnerships in research projects or consortia, but also other economic activities.

Innovation & exploitation during the project

The innovation and exploitation possibilities explored during the three years of the project are the following:

Year 1:

- During the first year, AYTOSAN collaborated with the M-Sec project partners, in particular with UC owners, in the definition of the different pilots, and with those in charge of the municipal services, in order to find a balance between the project objectives and the needs of the city.
- In the case of pilot 1, continuous meetings were held with TST (UC1 owner), the municipal environmental service, the municipal services of parks & gardens as well as industrial engineering teams to present the project and start working on the pilot definition. AYTOSAN started by choosing the location in the city for the IoT devices deployment (Las Llamas park) and then, started the analysis of the situation of the devices within the park. In addition to the IoT devices, it was proposed to install QR codes at different spots in the park to provide information about the flora and fauna in an interactive way. Both types of information





would be available through a user-friendly website. In parallel, AYTOSAN started working on ways to involve citizens in this pilot.

- For pilot 2, regular meetings were held with WLI (UC2 owner), the municipal service of Social Services, as well as with Atenzia, the company in charge of the telecare service, to introduce the M-Sec project and start discussions about pilot definition, including among other tasks the selection of IoT devices to be installed, the participants' requirements as well as the end-users' recruitment and involvement.
- In the case of cross-border pilots, preliminary discussions were held with the UC owners to start defining the pilots.
- Finally, the municipal DPO has been involved from the beginning of the project to ensure compliance with the GDPR in each of the pilots.

Year 2:

- During the second year, AYTOSAN focused their efforts on a more detailed definition of the pilots to be implemented in Santander.
- In the case of pilot 1, regular meetings including visits to Las Llamas Park were undertaken to analyse in the field the locations of the IoT devices as well as the QR codes. In addition, the municipal environmental service provided information and pictures of the flora and fauna of the park. The web site began to be designed with the collaboration of TST in the look & feel as well as the visualization of the content. The municipal DPO in collaboration with TST began the assessment of the pilot from the point of view of GDPR compliance as well as the elaboration of the required documentation (joint controller agreement and informed consent) started.
- For pilot 2, regular meetings were held with WLI, the municipal service of Social Services and Atenzia to fine-tune the pilot, on aspects such as the IoT devices to be installed in users' homes, the configuration and functionalities of the Senior Care platform and end-users recruitment. An essential aspect of this pilot is GDPR compliance, whereby the DPOs of the three entities (WLI, Santander City Council, and Atenzia) collaborated in the assessment of the pilot and started preparing the required documentation (co-controller agreement, Data processing agreement, and informed consent).
- For cross-border pilots, AYTOSAN have participated in discussions about their definition as well as the assessment of compliance with the GDPR and APPI.

Year 3:

- During the third year, the final setup of the pilots was finalised and pilots launched. The Santander city council has gained some expertise in aspects such as GDPR and APPI regulations, website development, Blockchain and smart contracts knowledge and mobile apps testing.
- In pilot 1, once the GDPR documentation was completed and signed by the involved parties, the IoT devices and QR codes were installed in Las Llamas Park. The website was also tested with a small group of users, in November 2020. Based on the participants' feedback, work was done to improve the website, especially the display of environmental measurements, and to test the IoT devices in order to launch the second phase of the pilot.
- For Pilot 2, once the GDPR documentation was completed and signed by the involved parties, the IoT devices were installed at end-users' homes and the monitoring of their activity at home started through the Senior Care platform, as the pilot was launched in September 2020. At the end of the first phase of this pilot, end-users' feedback was collected and has been taken into account to improve the initial





solution, which was tested during the second phase of the pilot. In parallel, follow-up meetings have been held between the involved parties, working together to resolve any incidents.

- In pilot 4, while specifying the details of the cross-border pilot, close collaboration was established between Santander City Council, CEA, Keio University, and NTTE in the GDPR compliance, jointly preparing the required document (Representative Agreement) for the use of the Japanese app (Smile City Report app) in Santander. In parallel, Santander city council worked closely with Keio University to translate, adapt and test the app in Santander, before launching the pilot in both cities.
- In pilot 5, AYTOSAN have contributed to the pilot definition discussions, as well as to the recruitment of participants. In addition, Santander has offered the city data available on its open data platform to be integrated into the M-Sec Marketplace with the aim of enriching it and attracting a larger number of participants.

Innovation & exploitation after project conclusion

Once the project concludes, Santander city council intends to work on the following elements to capitalize on the developments achieved during the M-Sec project execution:

- AYTOSAN's participation in this project contributes to the municipality's objective of building a more human city, centred on the citizen, where technology is not a barrier, but an engine to improve their quality of life by adapting solutions to different user profiles.
- The main results and lessons learned from the M-Sec pilots can be integrated in relevant municipal services:
 - Pilot 1 will make it possible to evaluate both the website and the deployed IoT devices as well as to assess whether there is interest to maintain them once the project ends.
 - Pilot 2 will allow a comparison of the current analogue solution of the telecare service with the digital solution proposed by WLI. An additional remark is that involving elderly people in such technological projects is quite complicated, but thanks to this pilot, this has been done successfully.
 - Pilots 4 & 5 will allow the analysis of differences and synergies between Europe and Japan when using the SCR app and the Marketplace in order to securely share pictures of their experiences in both cities.
- The project and its pilots will be further promoted in the forums which the city participates in (as it has been done during the third year of the project in events such as "Examples of blockchain application in public administration" organised by Blockchain Aragon and "How to make sure regulation helps and not hinders development of blockchain-based solutions" organised by Blockstart project), thus sharing AYTOSAN's experiences and reinforcing the concept of urban laboratory.
- Additionally, Santander municipal website includes a section dedicated to the M-Sec project, where general information of the project together with the description of M-Sec pilots is available, including also the videos of the pilots with Spanish subtitles and the Spanish version of the M-Sec comic.
- Finally, AYTOSAN will maintain contact with pilots' participants, for example, through dedicated meetings, consolidating a community of citizens interested in new technologies.

5.1.4 TST

TST (<http://tst-sistemas.com/>) is an engineering company specialized on custom design and manufacturing of IoT products and services. TST assists companies with transforming their ideas into innovative, profitable, and feasible market solutions, with main focus on Smart City, Smart Agrifood and Industry 4.0 business areas.





TST is a member of the CELESTIA Technologies Group (CTG), an international multi-technology group composed of more than 250 engineers and offices in several European countries. CTG is a merge of high tech SMEs sharing a common strategic vision: innovation and technology to change the business concept and therefore provide value contribution to clients.

TST's goal is to create cutting-edge and competitive products and services, helping the clients to reduce operating costs and time-to-market.

TST invests heavily in R&D activities, with focus on electronic systems and devices, wireless networks, and advanced computing. TST is also an active member of platforms and forums related to IoT and Smart Networks and Services, like the SME Working Group within the 5G Infrastructure Public Private Partnership (5G PPP), IoT Council, PostScapes, and FIWARE.

TST is an SME which acts as the project's technological partner in the Smart City of Santander within the M-Sec context. In the last few years, TST has devoted considerable effort and acquired certain relevance in the IoT field. IoT is one of the great technological expectations for the upcoming future. Not in vain, it is identified as one of the R&D priorities by the European Commission. Therefore, the way to exploit results derived from the work in M-Sec within those contexts is already paved.

The main exploitation of M-Sec results for TST comes from:

- Acquiring knowledge in novelties around IoT security aspects incorporated from the overall M-Sec concept.
- Developing future products that will introduce a novel security layer into the TST IoT devices portfolio.
- Establishing strong collaborations with consortium partners that may lead to open novel business opportunities both in Europe and in Japan.

Innovation & exploitation during the project

The innovation and exploitation possibilities explored during each of the 3 years included in the timeline of the M-Sec project are the following:

Year 1:

- TST studied the market trends, competitors' analysis, and state of art of the technologies employed within M-Sec, with main focus on IoT security challenges at device level.
- TST explored technologies that are relevant to the Use Case 1. More specifically, TST researched the European Commission position regarding Air Quality and Air Quality Monitoring in cities (i.e., Clean Air policy package 2013).
- TST researched the current technologies related to air quality monitoring as well as the work carried out in other H2020 project (e.g., hackAIR, Decode Project, iSCAPE).

Year 2:

- TST studied and evolved the security solutions to be adopted at device level. In this regard, the work was initially focused on the use of ST's Trusted Platform Module (TPM) with devices based on Raspberry Pi.
- Additionally, other alternatives for security enhancement were studied to be applied on sensors based on devices integrated on STM32-L4. For instance, the use of a specific module devoted to performing encryption processes over the measurements was analysed from the technical and economic point of view.





- Related to Use Case 1, TST with the support of Santander Municipality worked on a more detailed definition of the technical solution and its associated business case. In this regard, meetings and discussions with relevant Santander Municipality services took place.

Year 3:

- A pilot for Use Case 1 was implemented and deployed. It is expected to gather relevant feedback from users that will be used to identify the aspects most valued by them, as well as the points that require the implementation of improvements.
- The pilot has been used by TST to gain knowledge and experience related to data integrity, security, and privacy. The acquired skills have started to contribute to the definition of the next evolution of TST's IoT designs, based on IoT devices with built-in security mechanisms.
- Relevant synergies with other R&D projects where TST is participating to have been identified. These synergies are related to security mechanisms based on complementary technologies. For instance, within the MuSiC project (<https://penta-eureka.eu/project-overview/penta-call-2/music/>), TST developed a gateway with secure UART communications based on the segregation of resources and code in a secure area within the microcontroller to protect it against hacks.
- TST has been working with Santander Municipality in the economic feasibility analysis of the Use Case 1 that will help for the definition and update of the related business case.
- Finally, TST has participated in the evaluation of other Use Cases. For instance, TST has supported the evaluation of the Use Case 4 and the Use Case 5.

Innovation & exploitation after project conclusion

Once the project concludes, TST intends to work on the following elements to capitalize on the developments achieved during the M-Sec project execution:

- Implementation of improvements and industrialization of the IoT devices developed within the Use Case 1: environmental sensor and people counter.
- Evolution of TST's IoT products by integrating ST's TPM and other hardware modules for the segregation of trusted zones and encryption purposes.
- Presentations to other Smart Cities not involved in the project of the results obtained with M-Sec and of how M-Sec can transform their cities through the involvement of their citizens in the creation of healthy spaces.

5.1.5 CEA

CEA Leti is the largest French research and technology organization specializing in micro- and nanotechnologies. Dedicated to creating value and innovation for transfer to its industrial partners, Leti's 1,700 researchers strive to make our society smarter, healthier, more sustainable, and more secure. The scientific excellence and multidisciplinary expertise of its personnel are the foundation of Leti's offer to industry.

By creating innovation and transferring it to industry, Leti is the bridge between basic research and production of micro- and nanotechnologies that improve the lives of people around the world. Backed by its portfolio of 2,200 patents, Leti partners with large industrials, SMEs and start-ups to tailor advanced solutions that strengthen their competitive positions. It has launched more than 50 start-ups. Its 8,000m² of new-generation





cleanroom space feature 200mm and 300mm wafer processing of micro and nano solutions for applications ranging from space to smart devices. Leti's staff of more than 1,700 includes 200 assignees from partner companies.

The Sensor and Electronic Systems department DSYS is dedicated to research and development of innovative smart systems within consumer or industry related context. DSYS competences cover co-conception methodologies, design, security, integration and functional validation of the system in realistic environments using living lab and testbed infrastructure.

Within the M-Sec Project, CEA contributes to 1) Security at multiple layers, from devices to users' front-end and 2) on IoT middleware in the continuation of previous projects. During the M-Sec project, Kentyou (<https://kentyou.com/>) was established as a spinoff company centred on sensiNact exploitation and support. Part of the support for the integration of sensiNact in Use Cases is handled in this framework.

Innovation & exploitation during the project

Year 1

- Risks and threat intelligence on the IoT devices market to understand generic risks and critical risks per business.
- Comparison of security hardware counter-measures to risks, especially between proprietary implementations of secure elements (ST33, etc.) and standardized secure elements (TPMs).

Year 2

- Integration of TPM on very constrained devices (STM32L4) and higher-end products (Raspberry PI, STM32MP1) at lowest levels, aiming to target further IoT platforms of various scopes.
- Development of hardware-dependent software security technologies relying on TPMs, such as measured boot, Anonymous Attestations, platform integrity monitoring.
- Integration within embedded Linux Operating Systems to provide a reference design for upgrading security on legacy platforms such as popular raspberry pi. This reference design mitigates risks identified during year 1 without major hardware upgrade.

Year 3

- Development of a remote security platform, referred as "Security manager" including centralized security services optimized for IoT such as PKI, attestations, accounting, and identity federation
- Support for the security manager integration within Use Cases, especially with development of security proxies to wrap legacy applications.
- Integration of stronger security primitives in the sensiNact middleware.

Innovation & exploitation after project conclusion

In the project's afterlife, Kentyou is the obvious innovation and exploitation plan for sensiNact but also for other developments carried out with CEA and partners, in relationship with the Urban Technology Alliance. As a company, Kentyou will be able to speed up sensiNact developments and customization for smart cities with direct access to the market.

On the other hand, CEA continues the development of its security assets in particular in the scope of IRT Nanoelec public/private partnership. Under this framework, CEA have strong collaboration with ST





Microelectronics, a major manufacturer in the silicon industry, in order to specify prototypes and proof of concepts. CEA has plan to transfer technologies developed during the M-Sec project, in particular the integration of the TPM on embedded platforms.

5.1.6 F6S

As a community builder and services provider, F6S has become the largest startup/SME community globally with over 3.5 million users (entrepreneurs, founders, investors, etc.), thus being very experienced in animating the innovators network.

F6S delivers more than €2 billion every year to startups and SMEs, with the leading CRM for deal flow, corporate challenges, structured programmes, startup services, corporate partnering, recruiting, government grants and free startup resources. F6S is also the leading platform for application management for commercial, corporate, government, university, and other accelerator programmes, helping more than 17,000 such initiatives worldwide.

F6S has also experience in managing and implementing H2020 projects in innovation, startup/SME growth, market and investment readiness, community building and other more specific areas¹⁰. This is applicable to the M-Sec project, where F6S is the Dissemination and Community Manager in the EU side, leading WP5 “GDPR, dissemination, exploitation and sustainability” activities, and aiming at:

- Coordinating the communication and dissemination activities at project and partner levels,
- Actively promoting the project activities,
- Disseminating the project outcomes to the target audiences and attract new stakeholders,
- Supporting the engagement with the target audiences,
- Organising the M-Sec online contest, and
- Building the M-Sec community.

In this sense, F6S will use the project results to provide additional value for its community and build new services/features that enable the scaleup of its users, particularly the F6S IoT Group (www.f6s.com/iot).

Innovation & exploitation during the project

The tasks delivered by F6S in the scope of WP5 ran throughout the whole duration of the project (3 years) and the innovation and exploitation possibilities explored by F6S are the following:

Firstly, F6S used the project results (mainly after year 2) to provide additional value for its community and enabling the scaleup of its users, namely the F6S IoT Group. All relevant results were shared within the F6S IoT Group and an additional M-Sec page (<https://www.f6s.com/m-sec/about>) was created in the F6S platform, to further disseminate M-Sec events, deliverables, the online contest and other relevant information (e.g., White Paper, Cookbook, etc.). With it, F6S also expected and was able to attract new users to its community and platform, interested in the M-Sec topics. A large community of 250+ event participants and online contest applicants was thus built since the beginning of the project, adding to the already existing one of the F6S IoT Group. F6S also supported the dissemination of the M-Sec Marketplace, bringing knowledge of its benefits to its users’ community. Additionally, F6S facilitated the building of a Slack community

¹⁰ For more information, visit F6S Innovation page: <https://innovation.f6s.com/>





(<https://join.slack.com/t/m-seccommunity/>), currently with 60+ users, for a closer engagement between M-Sec project partners and involved stakeholders with interest in the project, particularly those involved or interested in M-Sec Use Cases and the Marketplace that will continue to streamline after the project's end.

Through the project activities, F6S also aimed to support the expanding of the technical solutions developed through the establishment of international collaborations, which are expected to last even after the project's end. The focus was on smart cities initiatives and other H2020 projects in the fields of Big Data, IoT, Blockchain, etc. With Cyberwatching.eu, an H2020 project that compiles and provides visibility to other EU-funded research projects on cybersecurity topics, F6S was able to showcase the technical results of the M-Sec project, share events and update the community on its Use Cases implementation, and be part of that community through the European Project Radar (<https://radar.cyberwatching.eu/radar>), "Project of the Week" Initiative¹¹ and visibility at events, among others¹². A long-term collaboration was also established with StandICT.eu, an H2020 project that supports the European presence in international ICT standardisation bodies, for exchange of relevant information and opportunities. F6S integrated 3 public discussion groups of their EU Observatory for ICT Standardisation on behalf of M-Sec – smart cities, IoT and cybersecurity – and shared with over 1000 users the main results and achievements of the project.

Other connections were also established with H2020 project BlockStart that supports blockchain adoption in Europe, the EU Blockchain Observatory and Forum, Japanese smart city initiatives such as the Takamatsu Smart City Initiative, and joint EU-Japanese initiatives such as EJEa, the European-Japan Experts Association. With these activities, F6S aimed at maximizing the direct dissemination and awareness of the project's achieved results within the European and Japanese industrial and academic sectors.

Moreover, F6S also helped reaching out to tech startups, the academic community and IoT innovations towards the adoption and/or development of M-Sec project findings that supported the creation of new business ideas that addressed smart cities challenges, through the promotion of an online contest. The M-Sec online contest was a space in which developers, entrepreneurs, startups, data scientists, University students, research community and persons interested in making their city a better place gathered to develop, in a collaborative and interdisciplinary way, a business idea that made the cities of Santander and Fujisawa more efficient, intelligent, sustainable, and secure.

Finally, as WP5 leader, F6S also supported the implementation of other partners' exploitation plans.

Innovation & exploitation after project conclusion

Once the project concludes, F6S intends to work on the following elements to capitalise on the developments achieved during the M-Sec project execution:

- Being the dissemination partner, F6S is not as involved in the Use Cases as the technical partners. Therefore, it is not directly contributing to technology advance within the M-Sec scope. Nonetheless, careful attention will be given to the technologies used and developed, to understand if an online community such as F6S could adopt them. In fact, F6S is particularly interested in exploring blockchain and security related solutions, as further improvements to its services/features. Depending on the

¹¹ For more details, visit M-Sec page as "Project of the Week": <https://cyberwatching.eu/services/catalogue-of-services/project-week-m-sec>

¹² For more details, visit M-Sec page: <https://www.cyberwatching.eu/projects/2636/m-sec>





technology which could be adopted, and in case there is interest, the F6S tech team would take the lead on the conversation into a marketable service within the platform, directly containing the M-Sec partner(s) involved.

- Growth in the Japanese market is a relevant component for the exploitation plan. With the engagement in an EU-Japan collaborative project, and this being the first time, F6S expects to gain cultural knowledge and proximity with Japan, which can further allow to communicate easier and more adequately the value of the F6S platform to Japanese companies, municipalities, Universities, and tech transfer offices (currently with a low participation), and therefore foster corporate innovation and connections between innovators, researchers, corporates, and cities. For this goal, F6S can make use of its corporate challenges service.
- Based on the good relations F6S had with the other project partners during the project's implementation, F6S expects an openness to potential future collaborations that may complement the value proposition developed by M-Sec and take advantage of F6S access to a global community of tech startups, entrepreneurs, investors, etc.

5.1.7 NTTE

The Nippon Telegraph and Telephone Corporation East, commonly known as NTTE, is a Japanese telecommunications company headquartered in Tokyo, Japan (<https://www.ntt-east.co.jp/en/>) NTTE is the fourth largest telecommunications company in the world in terms of revenue, as well as the third largest publicly traded company in Japan

NTTE is strongly committed to the notion of corporation as members of society, always striving to be a “good corporate citizen”, contributing to society actively in a variety of ways. As part and parcel of the local community, NTTE shares the same feelings and grows along with the community, working to create a better future. NTTE will continue to carry out these activities, focusing on themes specific to local communities, and will play a role as a good corporate citizen.

As a contribution to development assistance efforts by the Japanese government, NTTE has been carrying out international cooperation in the telecommunications field for more than 40 years. By sending engineers and transferring technologies to countries in need of assistance and accepting trainees from those countries, NTTE helps them to improve network quality, extend telephone services to all areas, and build up their own supply of skilled personnel. In return, NTTE has received numerous commendations and certificates of appreciation from both the assisted nations and the Japanese government.

Innovation & exploitation during the project

The innovation and exploitation possibilities explored during the three years of the project are the following:

Year 1:

- During the first year of the project, NTTE explored the use cases in each of the pilot cities based on the results of the analysis of the issues faced by the stakeholders and citizens of the area, taking into consideration the type of data to be handled and how to protect them with the consortium partners. In addition, the definition of the requirements for the field trial was discussed to plan for testing and to verify the use cases developed, stakeholder engagement plan, data management plan, and ethics plan.





- For Use Case 5, an analysis of the current marketplace was conducted with the aim of providing a solution that would meet the business side and user needs.
- Meetings were held with potential stakeholder groups and municipalities in order to identify feasible field trial scenarios for Use Cases 4 & 5.

Year 2:

- In the second year, NTTE continued to the evaluation of use cases, especially the cross border use cases, and tried to evolve them.
- While developing Use Case 5, NTTE gained knowledge on blockchain technology for data tamper protection, in line with data protection and integrity requirements, and along with this, also gained expertise in developing a safe and secure marketplace that complies with both GDPR and APPI regulations.
- In order to introduce M-Sec to various bodies, discussion on how to promote effective proposal activities to appropriate bodies were held in cooperation with consortium partners.

Year 3:

- During the third year, implementation between the M-Sec marketplace and each use case has been in progress to transfer the non-personal data collected from each use case to the marketplace.
- Meetings were held with various organizations to disseminate M-Sec. Activities were also carried to obtain field trial participants for Use Cases 4 & 5.
- The first field trial of UC4 was implemented with Jazz Meeting Event in Fujisawa city to evaluate what benefits the application would bring to citizens' life.
- In addition, in order to respond to the current pandemic, regular meetings were held with municipalities and stakeholders to update scenarios for the implementation of field trials.

Innovation & exploitation after project conclusion

Once the project concludes, NTTE intends to work on the following elements to capitalize on the developments achieved during the M-Sec project execution:

- Propose the secure platform built by M-Sec project to the smart city projects in Japan and overseas for horizontal deployment.
- Propose to use this achievement for ICT-led proposals in Japan's growth measures after the pandemic.
- Put efforts to maintain superiority in the blockchain business, which is expected to grow in the future, by constructing a secure blockchain foundation and its applications and services.
- Contribute to the solution of social issues and realization of SDGs, etc. as the NTT Group by implementing the smart city.

5.1.8 KEIO

Keio has a proud history as Japan's very first private institution of higher learning, which dates back to the formation of a school for Dutch studies in 1858 in Edo (now Tokyo) by founder Yukichi Fukuzawa. Since the school's inception, the students of Keio have risen to the forefront of innovation in every imaginable academic field, emerging as social and economic leaders. Based on the knowledge and experience of outstanding faculties, today's Keio students strive to develop the leadership qualities that will enable them to make valuable contributions to tomorrow's society.





Keio University has taken a great role in research and development in Japan. In 1990s, Keio University took initiative of the next generation micro-kernel technology project. In the area of ubiquitous computing research, the Ubiquitous Computing Laboratory at Keio University (hereinafter referred to as UBILAB/KEIO) joined the Ubilab project and the CUBIQ project funded by the Ministry of Internal Affairs and Communications and contributed to the development of core technologies in creating ubiquitous services and applications. UBILAB/KEIO has been developing both hardware and software systems such as smart space laboratory, smart living room, smart corridor, smart furniture and so on. Since 2010, it has been leading and actively participating in a number of national research projects related to IoT, AI, and Smart City.

As a research institute which is not for profit, KEIO will use the project results as follows:

- Through its participation in M-Sec, KEIO aims to develop innovative mechanisms that may be offered to the open source community. Since KEIO is a non-profit Academic Research Body, all related results will be released as open source contributions under Open Source licenses (more specifically, permissive licenses, as they are not restrictive licenses and can be used to create a proprietary good, allowing a commercial exploitation and ensuring high impact).
- For education in Faculty of Environment and Information Studies, KEIO will design a lecture course for bachelor students through which students can learn about IoT security, data trustworthiness, mechanisms for these purposes, blockchain, and sensor data marketplace.
- To foster young researchers, KEIO exploits the results in order to connect them with Master and Ph.D programme theses as well as the creation of new training courses, for the active engagement of young researchers in a multi-cultural and highly innovative environment.
- For further research advancement, KEIO will leverage M-Sec results as the basis of large-scale data distribution platform. In current and future research projects, including joint research projects with industry, academia, and governments, the M-Sec platform will be used to transfer sensing data from the edge-side to the user-side securely and with trust.

Innovation & exploitation during the project

The innovation and exploitation possibilities explored during the three years of the project are the following:

Year 1:

- During the first year, KEIO clarified the security issues inherent in distributed IoT systems observing KEIO mobile sensing platform as an example.
- It also revealed the privacy issues existing in image-based smart sensing systems, which capture the world using cameras, process the images using AI, or transfer the images to a cloud system.
- KEIO triggered a collaboration with YNU regarding IoT security mechanism to build secure KEIO mobile sensing platform, and developed GANonymizer, a mechanism an images anonymization tool.
- KEIO started actively presenting the M-Sec project to its collaborators, thanks to the availability of the initial demonstrators.

Year 2:

- During the second year of the project, KEIO continued evolving their assets, including SOXFire and GANonymizer, which are related to secure mobile sensing platform and trustworthy participatory sensing.





- During the specific development, KEIO has created publications and incorporated the specific technologies into its post-graduate courses and PhD research programme.
- KEIO started the design and implementation of pilot studies for Use Case 3, 4, and 5 with active discussion with the Fujisawa local government, end users, and other stakeholders.

Year 3:

- During the third, and last year of the project, KEIO implemented pilots for Use Case 3, 4, and 5 by collaborating with YNU, TST, and others. The implementation includes the bridging system between publish/subscribe and blockchain systems, and that between participatory sensing application and the M-Sec marketplace.
- Various webinars and dissemination events took place where the pilots with the secure SOXFire, secure mobile sensing platform, and smart city report application were presented and demonstrated.
- PhD research activities have been carried out with the help of the specific technology assets.

Innovation & exploitation after project conclusion

Once the project concludes, KEIO intends to work on the following elements to capitalize on the developments achieved during the M-Sec project execution:

- Propose the secure platform built by M-Sec project to the smart city projects in Japan and overseas for horizontal deployment.
- Propose to deploy Secure SOXFire and Secure Mobile Sensing Platform for local government work, such as road surface monitoring and garbage amount analysis, through joint research projects with them.
- For education in the Faculty of Environment and Information Studies, KEIO will design a lecture course for bachelor students through which students can learn IoT security, data trustworthiness, mechanisms for these purposes, blockchain, and sensor data marketplace.

5.1.9 NTTDMC

NTT DATA INSTITUTE OF MANAGEMENT CONSULTING, Inc. (hereinafter, NTTDMC) has taken it as their mission to enrich society. In keeping with this mission, NTTDMC have thus far provided high-value added knowledge and intelligence to meet diverse wants and needs, through our consulting activities.

Meanwhile, the times continue to change. NTTDMC are seeing the rise of business models applying new technologies. The times also demand management to be adapted to internal and external changes in the social and economic environment, as well as organizational management geared for innovation. NTTDMC have constantly polished their skills and capabilities while bolstering approaches to such environmental changes.

Besides the construction of mechanisms for resolution of social issues in areas such as the building of a low-carbon society and fuller coordination in provision of community medical services, this may be exemplified by our pursuit of the latest methodologies and solutions to induce innovation, such as cloud computing, big data, social listening, and applied neuroscience.

NTTDMC is responsible of WP5 GDPR, dissemination, exploitation and sustainability. NTTDMC is leader of Task 5.2 (Exploitation and IPR activities) and Task 5.3 (GDPR compliance). NTTDMC is responsible to research the IPR and GDPR/APPI related issues regarding M-Sec project.





NTTDMC is constantly considering issues from the perspective of the future and proposes strategies and policies that could not emerge from thought on an extension of current lines. The M-Sec project, in that aspect, will give good opportunities for designing a new society, building the ICT- based future vision through our deep knowledge, experience.

NTTDMC's specific objectives in the course of this project are the following:

- To exploit planning activities.
- To standardize GDPR/APPI in smart city models.
- To define IPRs which will be used in smart city models.

Innovation & exploitation during the project

Year 1:

- During the first year, NTTDMC planned a general market strategy. NTTDMC defined the M-Sec solutions concept in the IoT platform market and value positions with partners.
- NTTDMC aggregated and organized general information on APPI and the elements of mutual recognition on APPI and GDPR.
- NTTDMC presented the M-Sec project plan at an external conference.
- NTTDMC discussed cross-border UC plans with partners to give influence to citizens in Japan and EU, which intend to include things worth spreading and sharing for future external Projects.

Year 2:

- Product Proposition of M-Sec was defined in a more clear way along with the competitors' analysis (listed future important competitor developers and theirs products).
- Year 2 also implied the development of the M-Sec framework that would support the provision of the different use cases.
- The development of the core platform and the different services for each of the use cases implied the creation of a series of digital assets that can be used to accelerate the development of solutions from third parties.
- NTTDMC executed a gap analysis between GDPR and APPI regulations in order to be able to develop in line to the requirements of data protection and integrity a secure and safe storage layer.
- NTTDMC defined main requirements for each Use Case to comply with APPI regulation.
- NTTDMC participated in the cross-border Use Case 5 so that this use case can operate and match specific law requirements.

Year 3:

- A pilot for Use Case 5 was developed and will be released in order for the M-Sec consortium to establish a feedback on what it works and what needs to be mended.
- NTTDMC researched how Use Case 5 can acquire a licence to deal with data transaction business on Japanese law.
- Competitive points and weaknesses have been defined in a more clear way along with the competitors' analysis (listed specific elements of competitors' products related to specific indicators).
- NTTDMC defined main requirements for each Use Case to comply with APPI regulation.





Innovation & exploitation after project conclusion

Once the project concludes, NTTDMC intends to work on the following elements to capitalize on the developments achieved during the M-Sec project execution:

- Establish a consulting methodology for the secure and open smart city sector as a consulting firm for the ICT public sector and provide a wide range of consulting services.
- Establish a methodology for dealing with GDPR in Japanese companies in the smart city related field and enrich the consulting menu.
- Establish a sustainable Japanese version of the smart city business model by applying business model studies using the Business field through PoCs etc. to the smart city business in Japan.
- Collaboration of smart city related and group companies which intend to develop their own smart city services.
- Participation in Projects with municipalities or the Japanese government by referring M-Sec project results and services.

5.1.10WU

Waseda University (WU) is a private, independent research university in central Tokyo, Japan, founded in 1882 (<https://www.waseda.jp/top/en/>). As a research-oriented university, Waseda is highly regarded worldwide in numerous fields, from the social sciences and humanities to science and technology. In this line, WU established the Institute for Advanced ICT Research in 2018. At this research institute, WU promotes research and development on cutting-edge ICT basic technologies that support the future ultra-smart society.

WU promotes research and development of basic technologies such as AI, big data, video and audio processing, ICN (Information Centric Network), security, 5G (5th generation mobile communication), smart IoT, hardware security and robotics. The goal is to realize an ultra-smart society in which QoL (Quality of Life) is improved by integrating these elements organically, and by promoting social implementation through collaboration with different fields such as agriculture, medical care, transportation, and electricity.

Waseda University is the leader of WP4 “Multi-layered Security technologies” along with its responsibility on Task 2.4 “Overall system validation and Evaluation” and Task 3.2 “M-Sec Architecture”, given its expertise in dependable and secure software engineering. In particular, WU worked on self-adaptation of smart city applications to maintain high-security levels in response to changes in the environment. WU also contributed to the analysis and design of the M-Sec platform architecture.

Based on this background and motives, WU’s objectives are the following:

- To broaden the evaluation in a continuum that will cover 360 degrees of the M-Sec ecosystem.
- To handle both technical and stakeholders’ evaluation perspectives.
- To apply development tools and methodologies to real smart city application development scenarios.

Innovation & exploitation during the project

Year 1:

- WU jointly worked with ICCS to analyse requirements of the M-Sec platform and design the first M-Sec architecture.





- WU conducted a survey of existing techniques and tools in the application-level security.
- WU explored possible integration of MTSA with other assets.
- WU conducted research on improving smart city application development techniques.
- WU presented research outcomes at international conferences.

Year 2:

- WU jointly worked with ICCS to review feedback to the first M-Sec architecture and refine the M-Sec architecture.
- WU conducted research on controller synthesis algorithms to improve efficiency
- WU presented research outcomes at international conferences.
- WU designed a prototype integration tool between MTSA and Node-RED.
- WU organized an international workshop related to smart city and gave a presentation on M-Sec.

Year 3:

- WU implemented an integration tool between MTSA and Node-RED.
- WU jointly worked with KEIO to identify an application scenario under UC 3.
- WU developed a demo application using MTSA, Node-RED, and Secure SoxFire.
- WU conducted research on controller synthesis algorithms to improve efficiency.
- WU presented research outcomes at international conferences.
- WU gave an M-Sec webinar on application-level security.

Innovation & exploitation after project conclusion

Once the project concludes, Waseda University intends to work on the following elements to capitalize on the developments achieved during the M-Sec project execution:

- Continue research and development on application development tools for secure smart city applications. The MTSA-NodeRED-SecureSoxFire integration developed in the M-Sec project provides a foundation for smart city application development. The integration will be used in other smart city-related projects at which WU will be involved in future.
- Publish conference and journal papers related to research outcomes achieved in M-Sec project.
- Continue joint research with M-Sec partners. For example, WU, Keio, NII, and ICCS started joint research for secure smart city application development during the M-Sec project. WU will explore further opportunities to apply the techniques and tools in other smart city applications in real cities.

5.1.11YNU

Yokohama National University (YNU) is one of the leading national universities located in Yokohama, Kanagawa Prefecture, Japan. It comprises five graduate schools and four undergraduate faculties. In October of 2014, using a grant for Promoting the Reform of National Universities, Yokohama National University established the Institute of Advanced Sciences (IAS). Based on the notion of “risk symbiosis,” the IAS has begun conducting research to develop the kinds of rational risk management needed in the 21st century and to help make society safe, vibrant, and sustainable. YNU has many achievements in national projects etc. as a leading research base for information and physical security research and development. It has participated in the Cabinet Office Strategic Innovation Creation Program (SIP) "Securing cyber security in important





infrastructure (2015-2019)", "Auto run system (2014-2018)", Ministry of Internal Affairs and Communications research "Cyber-attack prediction by international collaboration", research and development of prompt response technology (2011-2015), and NICT commissioned research "Research and development for practical use of Web-mediated attack countermeasure technology (2016-2020)".

In the M-Sec project, YNU has mainly contributed in WP4 "Multi-layered Security technologies". In particular, as the task leader for Task 4.1 "IoT security" and Task 4.2 "Cloud and data level security", YNU has worked on securing the IoT layer (sensor devices) used in the use cases as well as the sensor data. YNU has also contributed in other work packages and tasks providing information security expertise in general, and with security threats and risk management.

As one of the national universities of Japan, YNU's exploitation plan includes using the project results as follows:

- Collaborate and contribute to securing digital world with its research expertise.
- Contribute in the development of secure smart cities and societies.
- Develop multiple security solutions for M-Sec needs based on open source software.
- Establish mutually beneficial collaborations with M-Sec partners that may lead to future joint research projects, both in Japan and Europe.

Innovation & exploitation during the project

The innovation and exploitation possibilities explored during the three years of the project are the following:

Year 1:

- Utilized YNU's state-of-the-art honeypot system for research and analysis of different attack vectors on various IoT devices.
- Researched appropriate counter measures for data and asset protection, including Intrusion Detection System (IDS) and visualization tool.
- Collaborated with KEIO, TST, CEA, and ICCS for developing M-Sec requirements.
- Published and presented research outcomes in national and international workshops, journals, conferences, etc.

Year 2:

- Collaborated with KEIO, TST, and CEA for developing M-Sec security solutions.
- Developed IDS for the IoT sensor devices and implemented on the KEIO mobile sensing platform.
- Developed and implemented cloud-based visualization tool for security monitoring.
- Researched port knocking (stealth security feature) for protection from unknown threats.
- Provided guidance and conducted security threats and risk assessments for WP3.
- Explored possible integration of YNU's developed security solutions with other assets.
- Conducted pilot-based initial testing of implemented security solution.
- Analysed and fixed issues to improve the effectiveness of security solution.
- Presented M-Sec IoT and cloud layers in webinars.
- Published and presented research outcomes in national and international workshops, journals, conferences, etc.





Year 3:

- Demonstrated proof of concept in real-life scenario through the pilot-based testing of IoT device-level security with M-Sec developed security controls.
- Developed and tested stealth security feature for the protection from unknown threats.
- Conducted pilot-based testing of IoT cloud/data-level security using visualization tool.
- Led final threat and risk assessments for confirming fulfilment (mitigations), collaborating with partners.
- Mentored M-Sec online contestants and winners.
- Presented Secured Smart City Framework jointly with EU in webinar.
- Published research outcomes individually and in collaboration with EU partners in the national and international journals.

Innovation & exploitation after project conclusion

Once the project concludes, YNU intends to work on the following elements to capitalize on the developments achieved during the M-Sec project execution:

- Support the realization of a secure IoT society through information security research and development, both in Japan and abroad.
- Implement lessons learned from M-Sec project in further improving research related to information security among young researchers and students of Yokohama National University.
- Leverage M-Sec experience and knowledge to further broaden the joint research experience with M-Sec partners, public and private organizations, and research communities across the globe.

5.1.12NII

The National Institute of Informatics (NII), founded in 2000, is an inter-university research institute corporation and a research organization of information and systems. As an inter-university research institute corporation, NII has taken on the task of building and running essential research and education information infrastructures for Japan's academic community, including the SINET5 (a Japanese academic backbone network), a science information network.

The mission of NII, this unique national academic research institute, is to "create future value" in the new academic field of informatics. From the basic methodology of informatics to cutting-edge themes such as information security, artificial intelligence, Big Data and the Internet of Things (IoT), NII features in a wide range of research activities.

NII push forward with fundamental research valued from the long-term view as well as practical studies, aimed at resolving current social problems. Utilizing their services and knowledge, the M-Sec project was enhanced to stay competitive and sustain a platform compatible with of EU and JP regulations.

NII's specific objectives within M-Sec are the following:

- To exploit planning activities.
- To identify threats and countermeasures for smart city models.
- To support the security requirements of smart city models.





Innovation & exploitation during the project

The innovation and exploitation possibilities explored during the three years of the project are the following:

Year 1:

- NII defined system-level and user-level requirements (first version) of Use Cases with other partners.
- NII also analysed security threats of Use Cases with partners.
- NII planned to develop a tool which supports requirement analysis for typical threats and their mitigation.
- NII discussed the security analysis method with security researchers in Japan.

Year 2:

- The requirements of Use Cases were developed in a clearer way in year 2 and NII defined system-level and user-level requirements of Use Cases (final version) with partners.
- NII developed the application level security (first version) with partners according to the development of the M-Sec framework.
- NII developed “Security Analysis Tool” (SAT) based on security researchers discussions.
- NII analysed Use Case 3 “Secure and Trustworthy Urban Environment Monitoring with Automotive, Participatory, Virtual Sensing Technology” by using their security analysis method (misuse case diagrams) with Use Case 3 owners.

Year 3:

- NII completed the application level security (final version) with partners.
- NII analysed a pilot of Use Case 4 by using their security analysis method with Use Case 4 owners.
- NII has completed and provided SAT. SAT supports security requirements analysis by reusing typical threats and their mitigation approaches in a knowledge base. SAT is implemented as a plugin on astah* (a UML modelling tool developed by Change Vision, Inc).
- NII analysed Use Case 3 by using SAT tool again and checked the tool.

Innovation & exploitation after project conclusion

Once the project concludes, NII intends to work on the following elements to capitalize on the developments achieved during the M-Sec project execution:

- Establish a methodology for the secure smart city framework by applying security analysis using the SAT (misuse case diagrams).
- Collaboration of secure smart city related and group researchers which intend to develop the standard secure smart city framework.
- Participation in Projects with municipalities or the Japanese government by referring M-Sec project results.



5.2 Joint Exploitation

The overall M-Sec consortium is made of 12 partners, 6 from 4 different European countries (France, Spain, Greece, Ireland) and 6 from Japan. The consortium is represented by 3 large industrial groups: Worldline Iberia, NTTEast and NTTDMC; 3 research institutes: ICCS, CEA, NII, 3 universities: KEIO, YNU and WU; 2 SMEs: TST and F6S, in addition to 1 Smart City, Santander Municipality.

Due to the fact that almost 50% of the partners from the consortium are academia partners, exploitation is more related in re-using M-Sec components for further enhancement on future R&D Projects and for educational purposes, as well as for disseminating scientific results and participating in R&D related to their research line.

However, from the side of industrial partners, it should be highlighted that TST are interested in reusing some M-Sec exploitable assets as the device security ones in their own business and WLI are also interested in re-using the UC2 application with the security added by M-Sec for commercialization to customers segments such as Tele-assistance and Insurance companies.

The joint exploitation activities analysed by the M-Sec consortium can be classified considering the partners' profiles:

- Commercial exploitation of the M-Sec framework for a group of components or standalone components. M-Sec tools will be offered to companies such as innovative SMEs IoT providers to enable them to create their own turn-key solutions or integrate them into their solutions. On section 4.6 within this document, it is provided the updated version of the BMC for the Commercialization Business Model.
- Commercial exploitation based on the UCs developed to test the M-Sec framework (On section 5.3 "UCs driven Exploitation", the value proposition and Business Model Canvas per Use Case is provided).

For these two types of activities, the following steps will be followed by the prime contractor.

- Liaise with the customer in order to understand their needs and constraints.
- Propose a proper system configuration to be deployed and identify the developments which might be needed.
- Contact the associated technology partners, depending on the security modules to be used.
- Negotiate with each partner the price and terms for: a) the software licensing, b) the developments which might be needed, c) the subsequent operation and maintenance tasks.
- Present an integrated offer to the customer – and possibly negotiate further.
- Upon offer acceptance, manage the preparation and establishment of the main contract and subcontracts (to the M-Sec partners).
- Upon contract establishment, act as Project Manager / single-point-of-contact for the customer, supervising all tasks related to the deployment (and subsequent maintenance) of the M-Sec solution.

Beyond the above activities, M-Sec partners will also:

- Offer consulting services (GDPR & APPI compliance, innovative UCs and business models based on the lessons learnt from UCs, main IoT risks & threats, applicability of technologies such as blockchain, cloud, etc.).
- Continue participating in events to promote M-Sec outcomes (in e.g., conferences, workshops, seminars).
- Publish joint scientific articles or the UC outcomes in industrial journals.



To know the partners' willingness to participate in these joint activities, the exploitation team conducted a short questionnaire. As a summary most of the partners are willing to participate in Promotional Activities or they might become willing, specially in workshops and events participation. However, in terms of joint exploitation and due to the nature of most the organization from the consortium (non-profit institutions), the ways of collaboration would be more focused on academia or future R&D projects. The questionnaire outcomes are depicted below.

- *"After the project conclusion, will you be willing to participate in promotional activities of M-Sec?"*

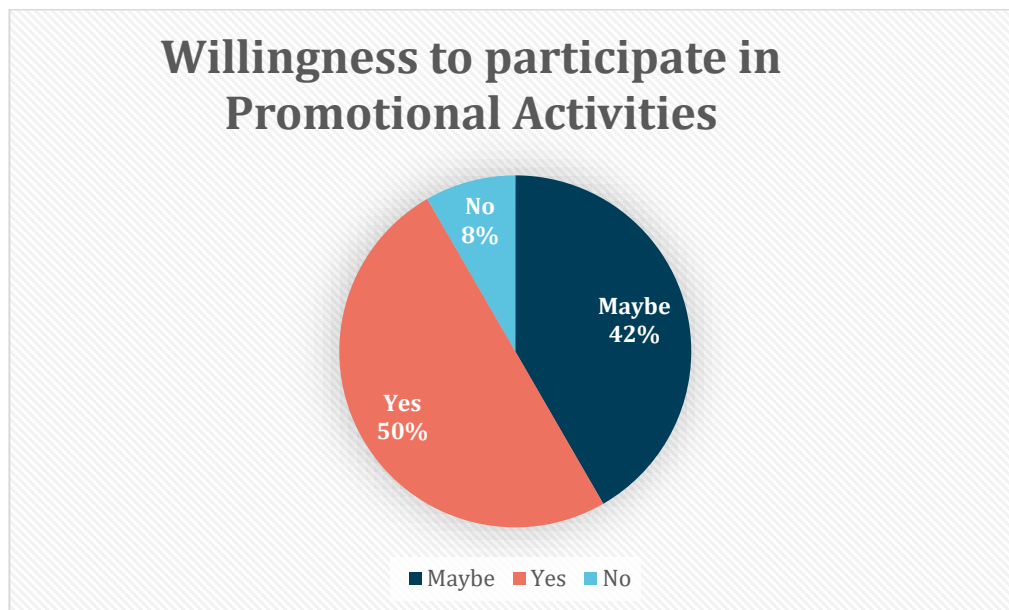


Figure 26. Willingness to participate in promotional activities



- “If above question is Yes or Maybe, in which ones?”

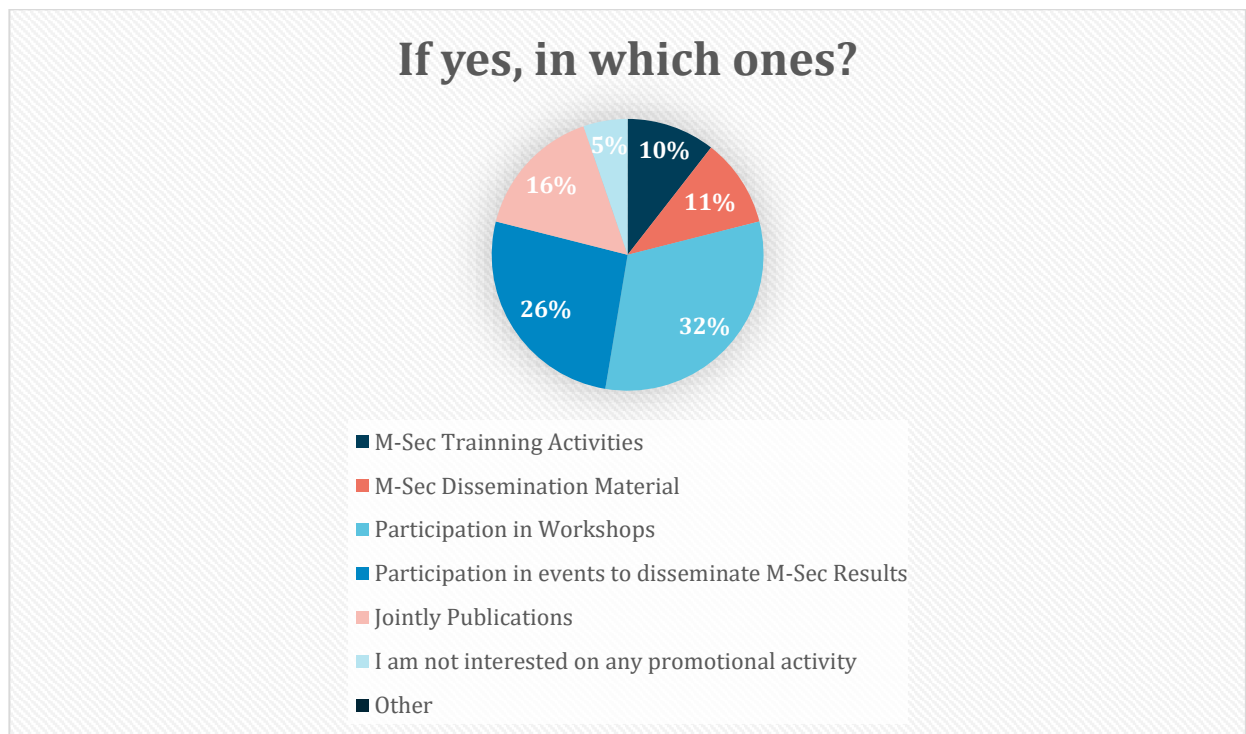


Figure 27. Promotional Activities

- “Are you currently interested in exploring joint collaboration with other partners from the consortium to exploit some M-Sec assets or UCs in a commercial way?”

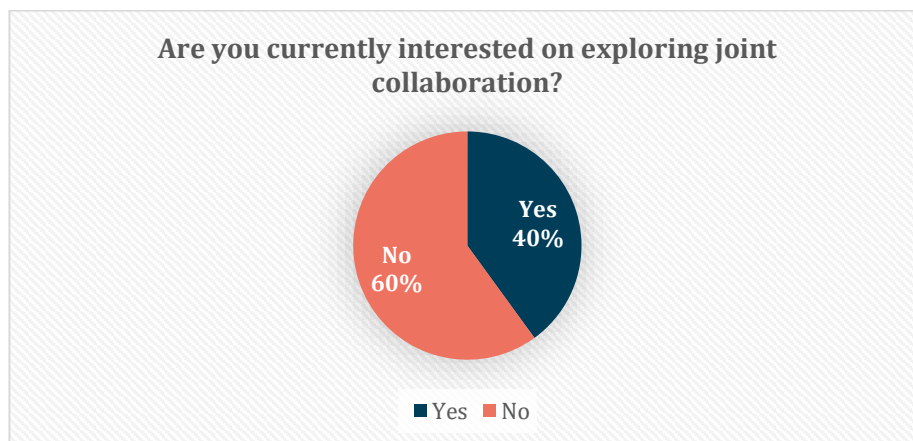


Figure 28. Jointly Collaboration

Partners who replied Yes, are interested mainly in the IoT environmental devices, low level security components and software for IoT devices and gateways and MTSA-NodeRED-secureSOXFire integration.

- “The European Commission expects the consortium partners to engage in joint exploitation, if commercial activities arise after the project conclusion. For this, a Memorandum of Understanding (MOU) is usually signed by partners in order to cover topics such as IPR, ownership, etc, Would you be willing to sign an MOU for future joint exploitation?”



Would you be willing to sign a MOU for future joint exploitation?

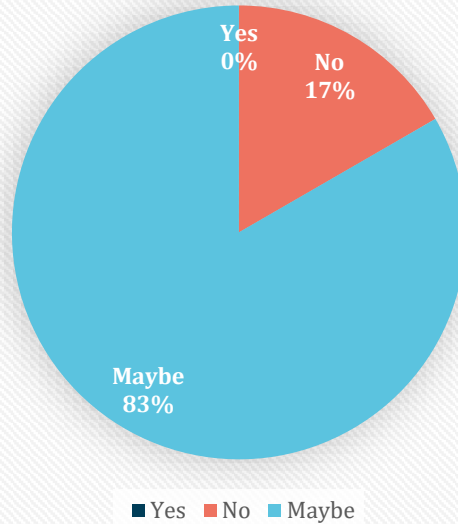


Figure 29. Willing to sign a MOU?

- *"In case of future collaboration opportunity in which your organization was not interested, would you sign a third party exploitation agreement with the M-Sec consortium partners involved in order to allow them use your assets (royalties, rewards, etc. would be negotiated) ?"*

Would you sign a third party exploitation agreement with the M-Sec consortium partners

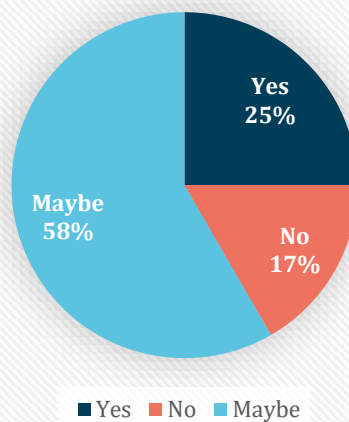


Figure 30. Willing to sign a third party agreement?





5.3 UCs driven Exploitation

In this section, the value proposition and the business model canvas are provided for each of the five different replicable use cases developed and implemented within the project for the purpose of testing the M-Sec Security Framework. A brief description of each one of the UCs is provided. In addition, a brochure has been created in order to show in a visual manner the problems/challenges addressed, the novel and unique proposition, technical components used, stakeholders groups targeted, and success stories and testimonies from end users extracted.

5.3.1 UC1: Secured IoT Devices to enrich strolls across Smart City Park

5.3.1.1 Use Case Overview

Use Case 1 is aimed at enriching the experience of visitors in Las Llamas park (Santander) by providing them with useful information, as well as trivia about its flora and fauna. In order to achieve this objective, five environmental monitoring IoT devices have been deployed throughout the park. These IoT nodes measure five different environmental variables: temperature, humidity, CO₂, volatile organic compounds, and noise. Besides, an innovative people counter device was developed and installed in the park to provide an estimation of the number of visitors in the park. Finally, nine QR codes are scattered throughout the park to provide interesting information about the biodiversity.

The information provided by the deployed IoT devices is relevant for not only citizens and tourists, but also for the Santander Municipality, since it can be used for programming actions in a more effective way.

Users have access to all the information, including the data provided by the deployed sensors, through the Park Guide application (see Figure 31). This is a web application that has been especially designed to facilitate the visualization of measurements. In this regard, measurements are presented in tables and in plots.



[Mi cuenta](#) [Cerrar sesión](#)

[Las Llamas](#) [Experiencia piloto](#) [Recorra el parque](#) [Dispositivos](#)





Figure 31. The Park Guide web application (Las Llamas Park – UC1)

For more information about the use case, a product sheet is provided, accessible from the [M-Sec website](#).

SECURED IoT DEVICES TO ENRICH STROLL ACROSS SMART CITY PARKS

HEALTHY SPOTS

SIMPLE, SECURE & SMART REMOTE PARK CONDITIONS & ACTIVITY MONITORING
REAL-TIME ANALYSIS AND QUICK ACTION WHEN FACING EMERGENCY SITUATIONS BASED ON ENVIRONMENTAL AND CROWD COUNTING SENSORS

GUARANTEE A SAFE ENVIRONMENT FOR OUR CITIZENS

HEALTHY SPOTS AND THE MAIN CHALLENGE IN THE PROCESSING OF SENSITIVE DATA

M-SEC AS A SOLUTION TO THE GREAT CHALLENGE IN PRIVACY & DATA SECURITY

UNIQUE VALUE PROPOSITION

- Non-intrusive (wireless sensor networks)
- Friendly (no technical skills required)
- Scalable (extensive to various cities, parks and locations)
- System Resilience
- End to End Security (data encryption with asymmetric public/private key, blockchain technology for data tamper proof, distributed data, access control)

FOR WHOM IT MAY BE USEFUL?

Are you an IoT provider looking for a partnership to expand your business?

Are you part of the Municipal Services and want to rely on innovative ways to react quicker than yesterday and plan beneficial actions for the community?

Are you a citizen and want to know more about how these types of solutions can help on your daily routines?

PILOT TESTIMONY

"I'm really interested in getting to know how M-Sec solves technical and security related problems, which are a real concern today in this kind of Internet of Things deployments. The idea is quite interesting and could have a positive impact on the city. Both from the citizens point, since it could help to avoid large gatherings and also thinking about having real data to compare how environmentally safe and friendly are different spots"

(end-user, Spain)

Figure 32. Brochure UC1

For further details about how UC1 and the park guide app works, a video has been created for this purpose, available in [Youtube](#).

5.3.1.2 Value proposition & Business Model Canvas

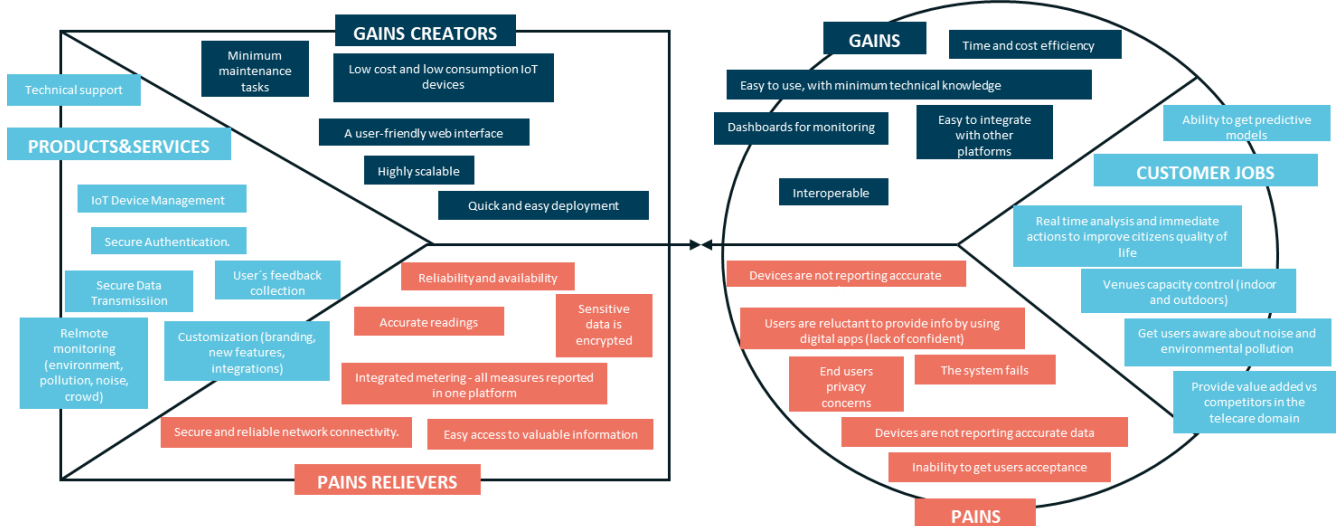


Figure 33. Value Proposition Use Case 1





| | | | | |
|--|---|--|--|---|
| Business Model Canvas | | Designed for: | Use Case 1 - Secured IoT devices to enrich strolls across smart city parks | |
| | | Designed by: | TST | |
| KEY PARTNERS | KEY ACTIVITIES | VALUE PROPOSITIONS | CUSTOMER RELATIONSHIPS | CUSTOMER SEGMENTS |
| <ul style="list-style-type: none"> - Municipalities (City Council + Concessionaire companies) and municipal services (CS1, CS2) - Telcos, as they provide connectivity services - European Union for funding and dissemination - M-Sec Consortium partners | <ul style="list-style-type: none"> - Evolve the demonstrator to a final product. - IoT devices adaptation for certification and industrialization - Website evolution by adding intelligence and processing features - Get feedback from stakeholders to possibly add more parameters or extend capabilities - Evaluate pilot with Ayuntamiento de Santander and prepare key messages to "sell it" - Start the service awareness and implementation processes - Raise investment for product commercialization | <p>VP1 (CS1-5): A B2B2C, SaaS-based, IoT platform featuring integrated components to enable environment, noise, pollution and crowd monitoring.</p> <p>VP2 (CS1-6): secure all aspects related to data access, data interception, data tampering attempts, IoT protection. Ensure data integrity and avoid man-in-the-middle scenarios.</p> <p>VP3 (CS1-6): ensure system resiliency (no single point of failure) and end user privacy</p> <p>VP4 (CS1-CS2): provide access to environment and crowd monitoring data to make analysis and predictions and get the citizens involved.</p> <p>VP5 (CS4-CS5): Collect real-time, IoT-based data on crowd counting to venues capacity control</p> | <ul style="list-style-type: none"> - Product Manager and Account Manager - Customer's sales agreements - Support tool for technical services to customers - Service customization (branding, new features, integrations) | <ul style="list-style-type: none"> - Municipalities and Public Administration services (CS1, CS2) - CS1: Environmental service - they offer this service to the citizens, get them establishing fixed routes and enriching them with environmental and pollution information - CS2: Tourist service - they can offer this service to the citizens and tourists, get them to know flora and fauna information in the park, as specific trees, birds, etc. They can also check the estimated number of people visiting the park to avoid the visit if it is too crowded. - CS3: Telcos - they sell their SIMs and communication services to Municipalities. Eventually, they also build a public service value proposition. - CS4: Recreational environments and tourist parks private businesses - they offer this service as an added value to their users, including in their apps the information about environment, pollution and estimated number of people in the different areas. - CS5: Events organizers companies (sports, concerts, congresses, etc) - valuable data to get analyzed and to be offered to the events attendees. |
| | | KEY RESOURCES | CHANNELS | |
| | | <ul style="list-style-type: none"> - Technical team to develop the demonstrator and evolve it to a product (IoT devices and app). - Communication roles (stakeholders, press, etc.) - Hosting infrastructure - Funding research to cover the evolution from pilot to product - Consortium governance and business model expertise | <ol style="list-style-type: none"> 1. Awareness: <ul style="list-style-type: none"> - Pilot with Santander Municipality & 1 CS1 and feedback from end users. Once we have results we move to the next phases. - direct meetings with existing partners to extend the pilot. - articles, brochures, blogs on how the service is much better than existing processes, social media, etc. - web marketing to lead interested users to an informative/call to action landing page 2. Evaluation: surveys and feedback programs via online and face to face. 3. Partners (via their sales force) 4. Delivery: deployment via outsourcing to local companies and the service via SaaS mode by TST 5. TST Sales - Business Development managers 6. After sales: Customer service | |
| COST STRUCTURE | | REVENUE STREAMS | | |
| <ul style="list-style-type: none"> - Employees salaries: product ownership / project management, communication roles, business roles (funding, business model definition and evolution), consortium governance roles and business model expertise - Cost for maintaining and evolving the platform (Product roadmap) - Dissemination costs (travel, tradeshows, articles, etc.) - Hosting infrastructure - Components cost for IoT devices production - Customer service | | <ol style="list-style-type: none"> 1. SaaS based business model leveraging on two phases: <ul style="list-style-type: none"> BUILD (Set-up phase): <ul style="list-style-type: none"> - A license fee for the Rights to Use the platform (including the IoT devices deployment) - An extra cost on branding customization (optional) - An extra cost on integrations of the platform with customer systems (optional) - An extra cost based on potential new features or new parameters required by customer (optional) RUN (operational phase): <ul style="list-style-type: none"> - A monthly fee based on the number of deployed sensors - An extra cost based on upgrades on the customer requirements | | |
| SOCIAL & ENVIRONMENTAL COSTS | | SOCIAL & ENVIRONMENTAL BENEFITS | | |
| <ul style="list-style-type: none"> - Energy consumption and environmental impact of the whole platform and its components, but lower than without IoT. | | <ul style="list-style-type: none"> - Smart business ecosystem development in the city - Reduced energy consumption | | |

Figure 34. Business Model Canvas Use Case 1





5.3.2 UC2: Home Monitoring Security System for ageing people

5.3.2.1 Use Case Overview

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

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

Worldline proposes Senior Care, an IoT platform that allows users to be monitored by deploying a series of sensors for the home (bed occupancy sensor, door/window sensor, movement sensor, etc.), as well as detecting emergency situations based on a series of previously configured rules and alerts, and thus giving immediate response. The solution aims to guarantee the security and safety of people who may be at risk due to factors of age, frailty, loneliness, or dependence.

Senior Care Assistance provides the following features:

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

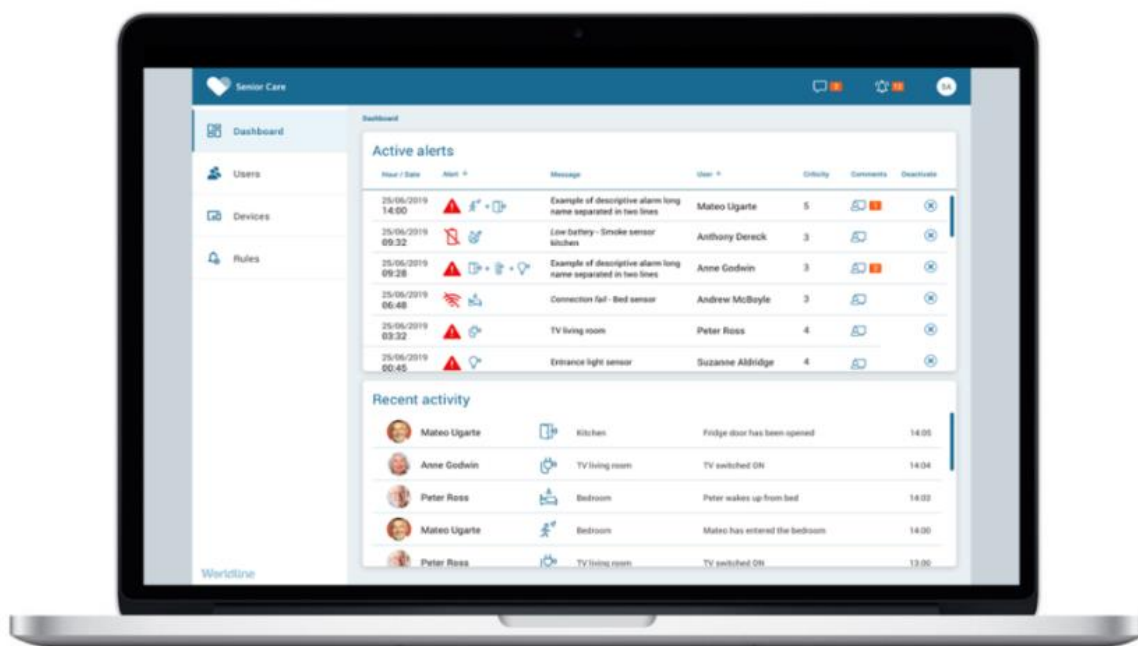


Figure 35. The Senior Care Web Application (UC2)





For more information about the use case, a product sheet is provided, accessible from the [M-Sec website](#).

HOME MONITORING SECURITY SYSTEM FOR AGEING PEOPLE

GUARANTEE THE SECURITY & SAFETY OF OUR ELDERLY

CIRCLE OF CARE

UNIQUE VALUE PROPOSITION

- Non-intrusive (wireless sensor network)
- Friendly (no technical skills required)
- Multi-Vendor (interoperate from the richness of the variety)
- Scalable
- System Resilience
- End to End Security (personal data encryption with asymmetric public/private key, blockchain technology for data tamper proof, distributed data, access control)

FOR WHOM MAY BE USEFUL?

- Are you a Tele-assistance provider and want to check a digital solution that replaces your current analogic solution?
- Are you an IoT Provider and want to partner to expand your business?
- Are you a telecommunication company and want to expand your portfolio?
- Are you the Municipal Services and want to provide innovative secured solutions for elderly?
- Are you a citizen and want to know more about how these types of solutions can help on your daily life?

PILOT TESTIMONY

"It is a service that does not require complicated installation, and provides very complete information on user habits"
(Atenea Teleassistance Services, Spain)

"I feel very safe, it is something simple that gives me a lot of peace of mind"
(end-user, Spain)

Figure 36. Brochure UC2

For further details about how UC2 and the Senior Care works, a video has been created for the purpose, available in [Youtube](#).

5.3.2.2 Value proposition & Business Model Canvas

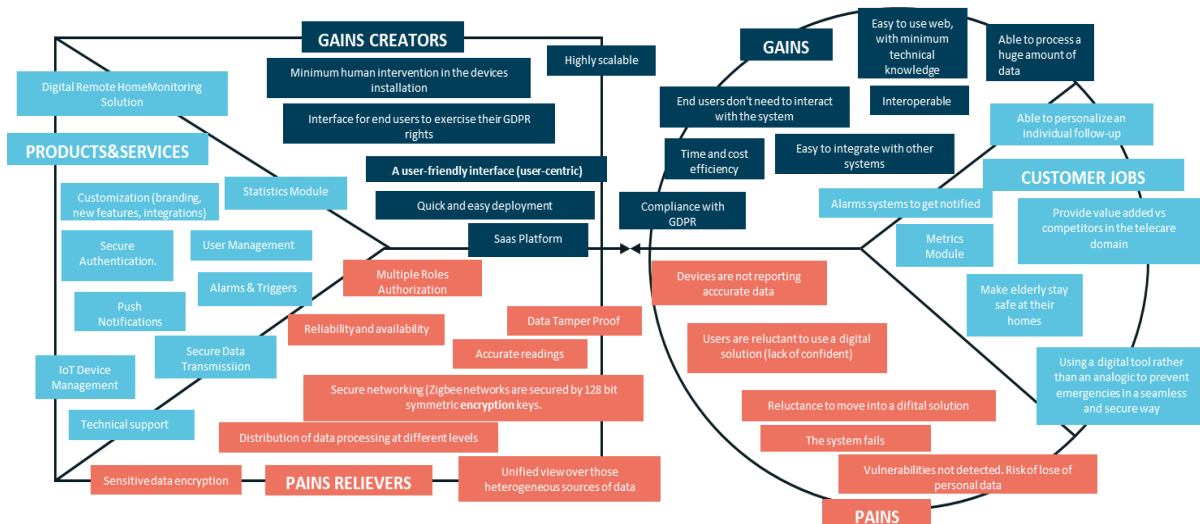


Figure 37. Value Proposition UC2





| Business Model Canvas | | Designed for: | HOME MONITORING SECURITY SYSTEM FOR AGEING PEOPLE | |
|---|---|--|--|--|
| | | Designed by: | Worldline | |
| KEY PARTNERS | KEY ACTIVITIES | VALUE PROPOSITIONS | CUSTOMER RELATIONSHIPS | CUSTOMER SEGMENTS |
| <ul style="list-style-type: none">- The CS1 should be the first members of the consortium, followed by some CS3 (particularly public administrations like local governments and city councils)- Hardware partners to provide sensors and devices- European Union for funding and dissemination- MSEC Consortium partners | <ul style="list-style-type: none">- Build the demonstrator and evolve it to a platform (Agile approach)- Get feedback from stakeholders- Generate awareness about Connected Care, M-Sec services and the project itself- Agree on a pilot with Ayuntamiento Santander and the initial pilot users- Evaluate pilot and prepare key messages to "sell it"- Start the service awareness and implementation processes- Raise investment for product commercialization | <ul style="list-style-type: none">VP1 (CS1-4): A B2B2C, SaaS-based, IoT platform featuring integrated components to enable tele-monitoring user-centric solutionsVP2 (CS1-6): Secure all aspects related to data access, data interception, data tampering attempts, IoT protection. Ensure data integrity and avoid man-in-the-middle scenarios.VP3 (CS1, CS3, CS4): Provide access to patient monitoring data to trigger accurate and adequate home care servicesVP4 (CS1-6): Ensure system resiliency (no single point of failure) and end user privacyVP5 (CS1, CS4): Collect real-time, IoT-based data on ageing citizens at their homes to provide accurate and rapid tele-assistance supporting services | <ul style="list-style-type: none">- Global Product Manager as SPOC- Self service on front end for users- Super admin users to support internally corporate customers- Email support for technical service.- Consortium management (i.e. committees)- Service customization (branding, new features, integrations with legacy systems)- API Rest for 3rd party developers | <ul style="list-style-type: none">CS1: Tele-assistance companies - they monitor users at home through IoT sensorsCS2: Telcos - they sell their SIMs and communication services to tele-assistance companies. Eventually, they also build a tele-assistance value proposition to these companies as a one-stop shop.CS3: Public Social Services - they offer this service to their citizen, mostly through service providers like CS1.CS4: Insurance - new business models based on personalization (e.g. pay-as-you-drive). This solution will enable new services and benefits based on client's habitsCS5: Research institutions (pharma, university, research centers, hospitals) - anonymization and aggregation of patients data to conduct trialsCS6: Businesses - Anonymized and aggregated data for a personalized offering for ageing segments |
| COST STRUCTURE | | REVENUE STREAMS | | |
| <ul style="list-style-type: none">- Technical partner cost for maintaining and evolving the platform (Product roadmap)- Personnel costs: product ownership / project management, communication roles, business roles (funding, business model definition and evolution), consortium governance roles and business model expertise- Dissemination costs (travel, tradeshows, articles, etc.)- Hosting infrastructure- Consortium creation and maintenance- Hardware (device and sensors) acquisition- Partners fees- Customer service | | <p>1. SaaS based business model leveraging on two phases:</p> <p>BUILD (Set-up phase):</p> <ul style="list-style-type: none">- A license fee for the Rights to Use the product (RTU)- An add-on fee based on branding customization (optional)- An add-on fee based on integrations of the platform with customer legacy systems (optional)- An add-on fee based on potential new features required by customer (optional) <p>RUN (operational phase):</p> <ul style="list-style-type: none">- A monthly fee for each platform user- A monthly fee add-on based on partners participation and hardware assignment (if not purchased by end user)- A monthly cap fee if a minimum number of users is not reached <p>2. API REST - price based on service consumption</p> | | |

Figure 38. Business Model Canvas UC2

5.3.3 UC3: Secure and Trustworthy Mobile Sensing Platform

5.3.3.1 Use Case Overview

This use case provides a client application that allows urban environment monitoring entities (for example local governments) to visualize spatially and temporarily dense environmental data such as air quality, temperature/humidity, garbage disposal amount, unimpaired road marks, etc.

The UC is based on the Keio Mobile Sensing platform that has been conducting demonstration experiments with Fujisawa City for more than 3 years.

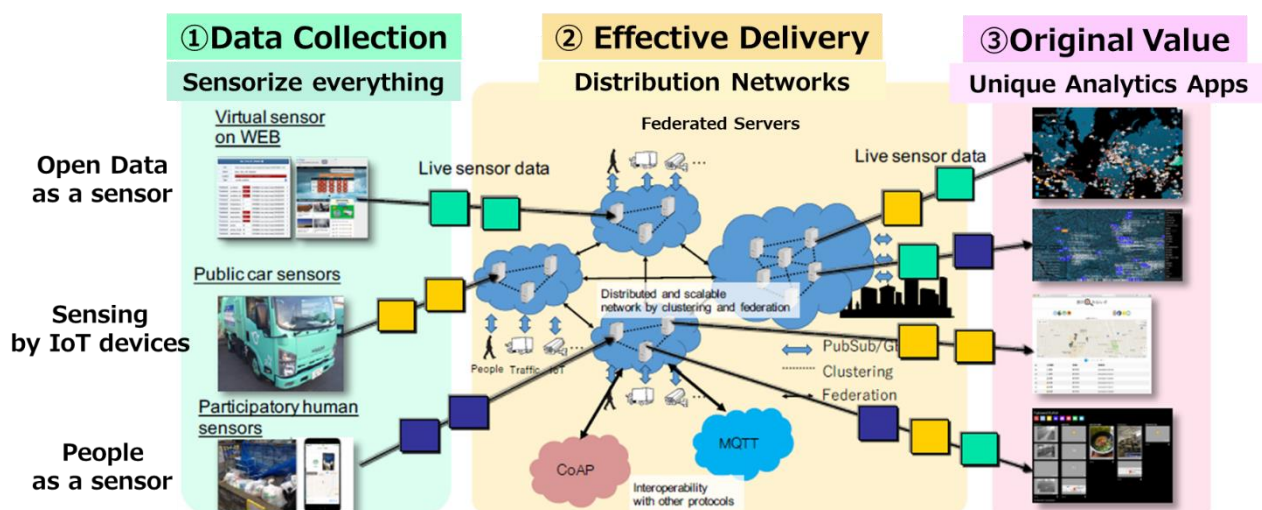


Figure 39. KEIO Mobile Sensing Platform (UC3)



For more information about the use case, a product sheet is provided, accessible from the [M-Sec Website](#).

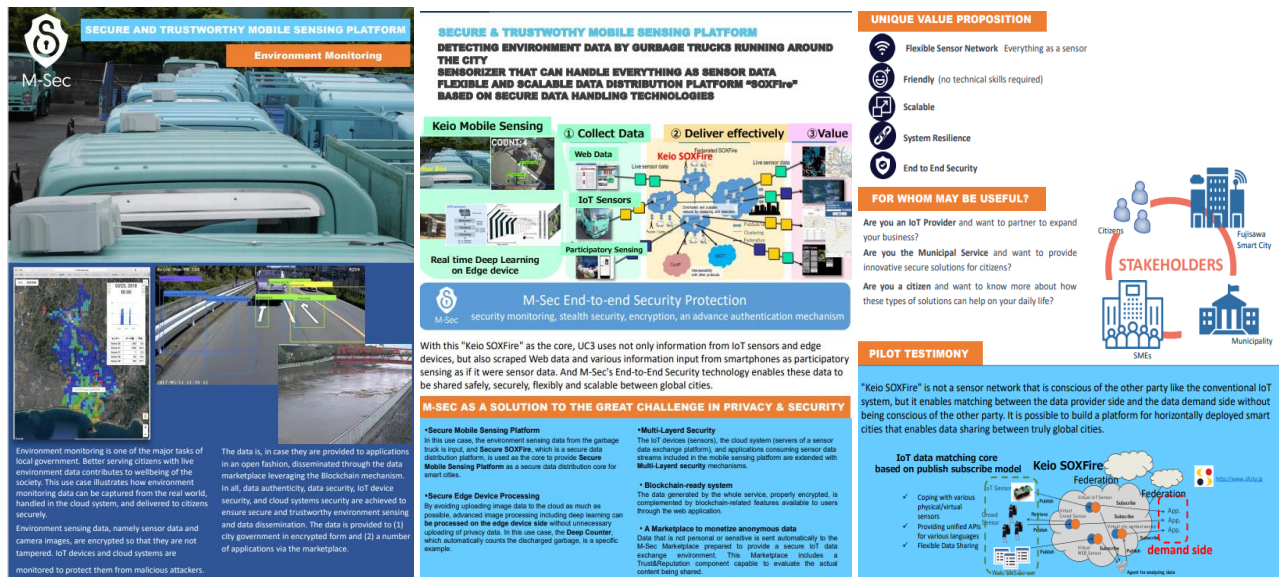


Figure 40. Brochure UC3

For further details about how UC3 and Mobile Sensing Platform works, a video has been created for the purpose, available in [Youtube](#).

5.3.3.2 Value proposition & Business Model Canvas

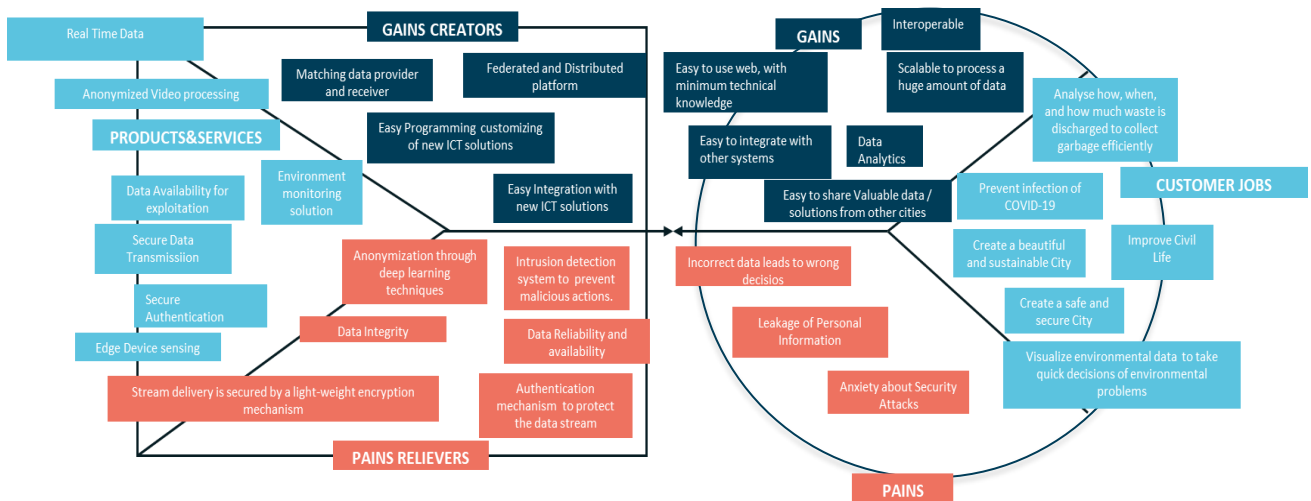


Figure 41. Value Proposition Canvas UC3





| Business Model Canvas | | Designed for: | SECURE AND TRUSTWORTHY MOBILE SENSING PLATFORM | |
|---|---|---|--|---|
| | | Designed by: | KEIO | |
| Following description is in the case of Garbage Truck sensing, but UC3 app is not limited only in this case. | | | | |
| KEY PARTNERS | KEY ACTIVITIES | VALUE PROPOSITIONS | CUSTOMER RELATIONSHIPS | CUSTOMER SEGMENTS |
| <ul style="list-style-type: none">- Fujisawa Recycle Coop- Fujisawa City- Sensing Data like air quality, road monitoring images, river monitoring images and so forth- Gathering IoT Sensing Data by sensor box installed on garbage trucks, road monitoring image Data by camera installed on garbage trucks, river monitoring image from open Data- MSEC Consortium partners- Restaurants in Fujisawa city- Sensing data like ventilation level- Gathering IoT sensing data by installed sensor box in Restaurants | <ul style="list-style-type: none">- Gathering data by IoT sensing, participatory sensing, open data analysis- Distributing data effectively by matching between data supplier and data consumer- Adding value by data analytic, AI processing and so forth- Supplying data, useful information as open data which everyone can access by Web browser or smartphone- Sharing the raw data and the results of analytic data | <p>VP1 (CS1-2): Realtime IoT sensing data in a way that is scalable</p> <p>VP2 (CS1-2): Automatically detection of road damage by deep learning analytics</p> <p>VP3 (CS2): Realtime river monitoring data from open web site</p> <p>VP4 (CS2): River monitoring data as a actual IoT sensing using sensorizer techniques.</p> <p>VP5 (CS3): Provide safety environment to citizen users in restaurants</p> <p>VP6 (CS3): Keep sustainable business activities for restaurant owner in COVID-19 environments</p> <p>VP7 (CS1-3) Data reliability and integrity. End to end transmission without disclose.</p> <p>VP8 (CS1-3) Vulnerabilities monitoring and detection 24x7</p> <p>VP9 (CS1-3) Data anonymization (delete personal objects in streaming)</p> <p>VP10 (CS1-3) Data anonymization and monetization for exploitation into the Marketplace</p> | <ul style="list-style-type: none">- Self Service as a data sharing by using web browser and smartphone apps. | <p>CS1: Fujisawa Recyde Coop</p> <p>CS2: Fujisawa City</p> <p>CS3: Restaurants in Fujisawa city</p> |
| | | KEY RESOURCES | CHANNELS | |
| | | <ul style="list-style-type: none">- M-Sec platform as a secure data distribution and exchanging platform- Samrtphone apps or Web browser as a frontend of M-Sec platform- Customer can refer usefuf information in real time- Edge devices for Deep Learning Analysis | <ul style="list-style-type: none">- Ideally, establishment of the channels structure including revenue mechanism enables sustainable business model is important.- There is just data sharing by web browser and smartphone apps.- There is not integrated channels yet. | |
| COST STRUCTURE | | REVENUE STREAMS | | |
| <ul style="list-style-type: none">- Maintenance cost of M-Sec platform, smartphone apps, server and so on.- System integration and maintainace cost of M-Sec platform | | <ul style="list-style-type: none">- There is not clear revenue stream yet as a sustainable business model. <p>The estimated ways to make revenue streams by providing users with developing service</p> <ul style="list-style-type: none">- Reduction of city officers resource cost- Reduction of partners' work effort by sharing necessary data effectively because there are lots of work by using traditional communication tool.- Reduce the human resource cost because there are lots of human resource cost | | |

Figure 42. Business Model Canvas UC3

5.3.4 UC4: Secure affective participatory sensing of city events

5.3.4.1 Use Case Overview

UC4 explores the possibility of secure sharing on citizens' affective information and information on the city. In the city, there are many different events occurring every day. As a means of detecting/sensing them, SmileCityReport allows people (citizens and possibly additional visitors) to report such events, from their own (human) perspective, with their mobile devices (e.g., smartphones). The user's photo-based report on a local happening will be shared among multiple users, after privacy protection processing of the taken photos takes place through an M-Sec component called GANonymizer. GANonymizer automatically deletes personal information from the picture taken with AI and Machine Learning Techniques. Moreover, the photo reports are securely shared only among defined "groups" in SmileCityReport so that only member users can view the photos of each other.



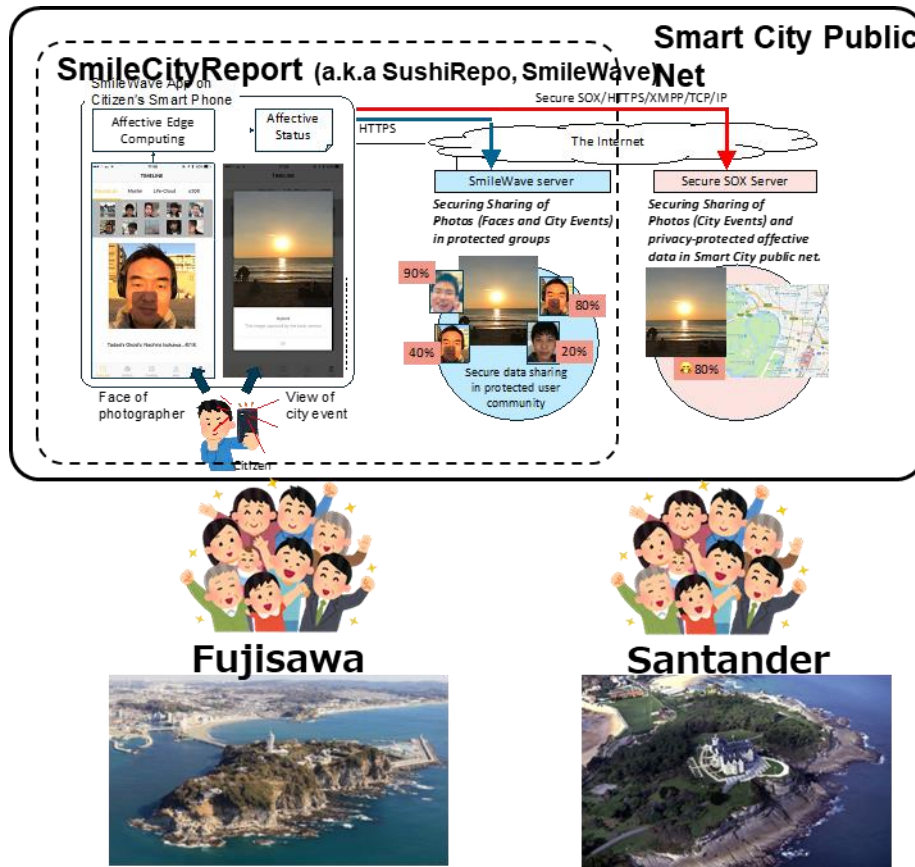


Figure 43. Smile City Report App (UC4)

For more information about the use case, a product sheet is provided, accessible from the [M-Sec Website](#).

Figure 44. Brochure UC4

For further details about how UC4 and the Smile City Report app work, a video has been created for the purpose, available in [Youtube](#).





5.3.4.2 Value proposition & Business Model Canvas

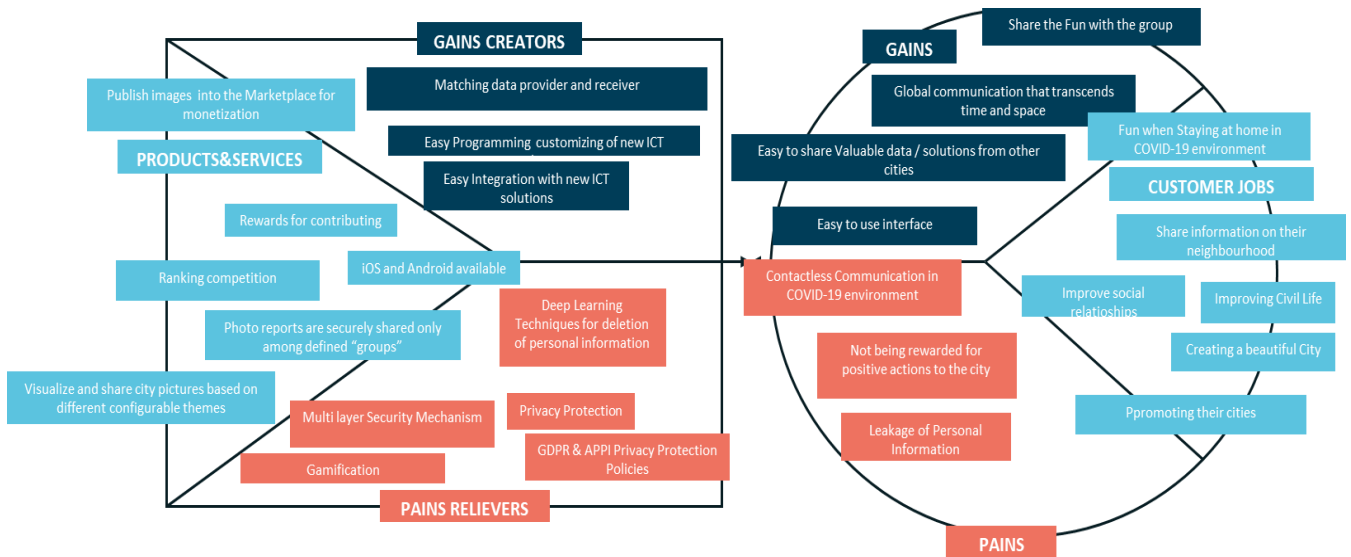


Figure 45. Value Proposition Canvas UC4

| Business Model Canvas | | Designed for: | SECURE AFFECTIVE PARTICIPATORY SENSING OF CITY EVENTS | |
|--|---|---|--|--|
| | | Designed by: | KEIO | |
| KEY PARTNERS | KEY ACTIVITIES | VALUE PROPOSITIONS | CUSTOMER RELATIONSHIPS | CUSTOMER SEGMENTS |
| <ul style="list-style-type: none"> - Municipalities (City Officer) - Citizens (Participatory sensing user) - Business person (shops, restaurants, events) - M-Sec Partners | <ul style="list-style-type: none"> - Supplying interesting information by smartphone application "SmileCityReport" via M-Sec multi layer security architecture - Distribute data effectively by matching between data supplier and data consumer - Adding value by data analytic, AI processing and so forth - Supply data, useful information as open data which everyone can access by "SmileCityReport" - Sharing the raw data and the results of analytic data as secure and trustworthy Hyper-connected Citizen Communication | <p>VP1 (CS1-3): Hyper-connected citizen communication by exchanging useful information depend on each purpose via M-Sec architecture including "SmileCityReport" as secure and trustworthy connection.</p> <p>VP2 (CS1) Exchanging images while preserving anonymization</p> <p>VP3 (CS1-3): M-Sec architecture including "SmileCityReport" as secure and trustworthy connection.</p> <p>VP4 (CS1): Providing secure and trustworthy data exchange platform</p> <p>VP4 (CS2-3): Take appropriate actions based on data shared to boost city wellbeing and promotion</p> | <ul style="list-style-type: none"> - Hyper-connected citizen communication by exchanging useful information via "SmileCityReport" (Android & iOS) | <p>CS1: Fujisawa Citizens, Santander Citizens</p> <p>CS2: Fujisawa City, Santander City</p> <p>CS3: Key partners who depends on each purpose</p> |
| | | KEY RESOURCES | CHANNELS | |
| | | <ul style="list-style-type: none"> - M-Sec platform as a secure data distribution and exchanging platform - "SmileCityReport" as a frontend of M-Sec platform - Customer can refer useful information in real time as secure and trustworthy Hyper-connected Citizen Communication. | <p>QR code promotion to install App</p> | |
| COST STRUCTURE | | REVENUE STREAMS | | |
| <ul style="list-style-type: none"> - Maintenance cost of M-Sec platform, "SmileCityReport", server and so on. - Reward cost according to points or M-Sec token | | <ul style="list-style-type: none"> - There is not clear revenue stream yet as a sustainable business model. Need further investigation with UC5 activities - The estimated ways to make revenue streams by providing users with developing service - Gathering Useful information including user's photo - Matching useful information publisher and subscriber - sell and buy at M-Sec marketplace | | |

Figure 46. Business Model Canvas UC4





5.3.5 UC5: Smart City Data Marketplace with Secure Multi-Layer Technologies

5.3.5.1 Use Case Overview

The M-Sec data marketplace is set up for citizens, companies and municipalities to trade data collected in other use cases and valuable datasets on the internet.

The screenshot shows the 'All the available sensors' interface. It includes a map of Europe with a red pin in France. Below the map is a table listing sensors for sale.

| Seller | Sensor ID | Sensor Type | Price (M-Sec Tokens) | First data at | Frequency | Map | Buy Data |
|---|-----------|-------------|----------------------|---|-----------|-----|--------------------------|
| 0c0f1b4ae53ae679b73bda97119cf48892b7c3c | 1 | temperature | 0.001 | Wed Nov 22 2017 17:57:35 GMT+0200 (EET) | 2 | | Buy Data |
| 0c0f1b4ae53ae679b73bda97119cf48892b7c3c | 2 | humidity | 0.001 | Wed Nov 22 2017 17:57:35 GMT+0200 (EET) | 2 | | Buy Data |
| 0c0f1b4ae53ae679b73bda97119cf48892b7c3c | 3 | pressure | 0.002 | Wed Nov 22 2017 17:57:35 GMT+0200 (EET) | 2 | | Buy Data |
| 0c0f1b4ae53ae679b73bda97119cf48892b7c3c | 4 | visibility | 0.006 | Wed Nov 22 2017 17:57:35 GMT+0200 (EET) | 2 | | Buy Data |

© 2019 M-sec Project

Figure 47. Marketplace Front-end (UC5)

For more information about the use case, a product sheet is provided, accessible from the [M-Sec Website](#).

The brochure is titled 'SIMPLE, SECURE & SMART DATA EXCHANGE' and 'A MARKETPLACE OPERATED IN A SECURE ENVIRONMENT CONSIDERING SECURITY REQUIREMENTS OF GDPR AND APPI'. It features a central diagram of the marketplace flow and several sections detailing its benefits and use cases.

GUARANTEE THE SECURITY & SAFETY OF OUR DATA

DATA EXCHANGE AND THE MAIN CHALLENGE IN THE PROCESSING OF SENSITIVE DATA

M-SEC AS A SOLUTION TO THE GREAT CHALLENGE IN PRIVACY & DATA SECURITY

UNIQUE VALUE PROPOSITION

- Friendly (easy-to-use interface, no technical skills required)
- Multi-Vendor (interoperate from the richness of the variety)
- Scalable
- System Resilience
- End to End Security (personal data encryption with asymmetric public/private key, blockchain technology for data tamper proof, distributed data, access control)

FOR WHOM MAY BE USEFUL?

- Are you a city and want to utilize specific data to improve your city?
- Are you a company and want to buy, get or sell specific data for your business?
- Are you a citizen and want to let your city utilize your data to improve the city?
- Are you a company who has many data from customers and want to sell a data securely?
- Are you an IoT Provider and want to provide a data exchange solution?

Figure 48. Brochure UC5

For further details about how UC5 and the Marketplace works, a video has been created for the purpose, available in [Youtube](#).





5.3.5.2 Value proposition & Business Model Canvas

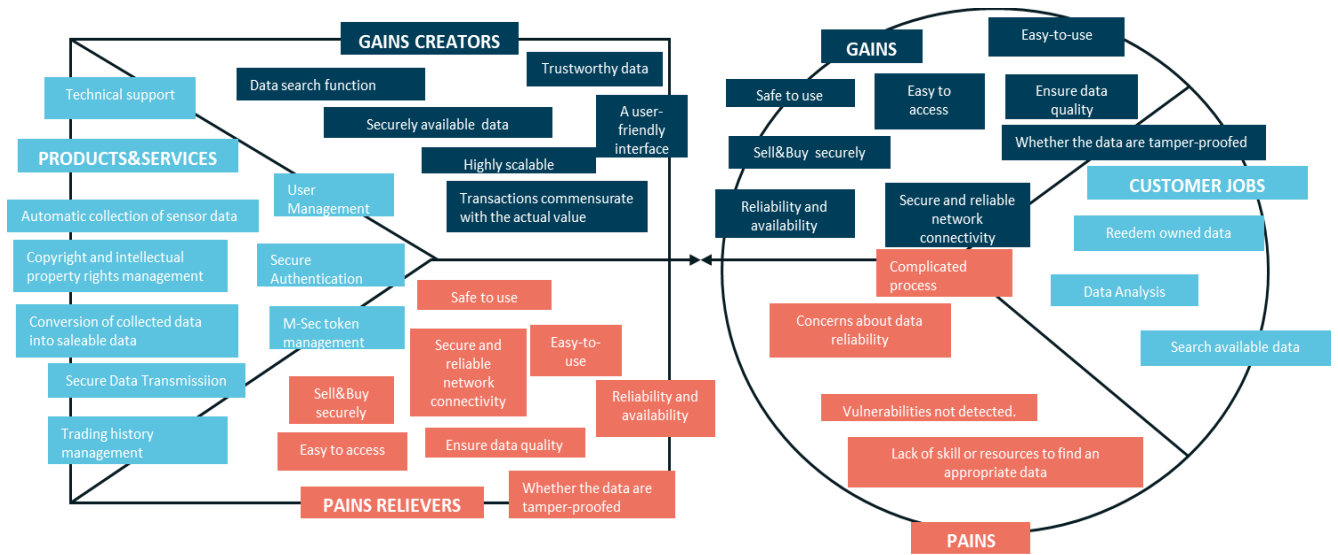


Figure 49. Value Proposition Canvas UC5

| Business Model Canvas | | Designed for: | SMART CITY DATA MARKETPLACE WITH SECURE MULTI-LAYER TECHNOLOGIES | |
|--|---|---|--|--|
| | | Designed by: | NTTE | |
| KEY PARTNERS | KEY ACTIVITIES | VALUE PROPOSITIONS | CUSTOMER RELATIONSHIPS | CUSTOMER SEGMENTS |
| <ul style="list-style-type: none">- M-Sec partners- Enterprises as buyers or sellers | <ul style="list-style-type: none">- Management of the platform, database, users data, update on security techniques | VP1(CS1): marketplace where they can get trustworthy data in a secure way when they want it VP2(CS1): Guarantee the data of quality. Not sure if the data they get is trustworthy, Not sure if the data is exchanged securely, Take time/labor to get data (interview, questionnaire, etc.) VP3(CS1): Can get trustworthy data efficiently VP4(CS1-2): Can be translated into their own languages VP5(CS2): Data monetization VP6 (CS1): Easy to search IoT raw Data VP7 (CS1): Real time raw data | <ul style="list-style-type: none">- To be trusted by managing and maintaining stable marketplace, Guarantee security- To be trusted by securing the individual information considering GDPR and PIPA- Web front end Marketplace | Buyer CS1: Enterprises who want to buy data (consulting firm, data analysis, marketing research, ad agency, municipality) Seller CS2: Enterprises or person who want to sell data (consumer, general company which has data, consulting firm) |
| | KEY RESOURCES <ul style="list-style-type: none">- Security know-how, blockchain, human resources (system design, management, support), multi-layered security technology, cloud server, payment system- KEIO smile city report- Santander Open Data- M-Sec Use cases raw data | | CHANNELS <ul style="list-style-type: none">- Trustworthy way, Recommendation from government, businesses,...- Authentication from credible organization, Exhibit in events organized by government or credible organization related to security. | |
| COST STRUCTURE | | REVENUE STREAMS | | |
| <ul style="list-style-type: none">- labor cost- service management & maintenance cost- hosting- license fee- promotion cost- R&D cost | | Customer's viewpoint: <ul style="list-style-type: none">- Buyer: Data sold by companies, Get data by taking their labor, Monetary reward for answers to questionnaires- Seller: Fee to participate in marketing research network User's viewpoint: <ul style="list-style-type: none">Buyer: Cheaper/more cost-saving than current processSeller: Can easily get money by selling data Revenue compositions ratio: <ul style="list-style-type: none">Marketplace membership fee (different membership level) (40%), Service charge (40%), Advertisement revenue (20%) Way to pay: <ul style="list-style-type: none">- prefer Credit card, QR payment to Cash | | |

Figure 50. Business Model Canvas UC5

5.4 Exploitation within ongoing and further R&D Projects and Educational Activities

Regarding educational activities, partners from Universities, like ICCS and KEIO, are leveraging the knowledge gained during the project to design and offer lecture courses for bachelor students through which students can learn about IoT security, data trustworthiness, mechanisms for these purposes, blockchain, and sensor data marketplace.





In addition, ICCS and WLI are involved in another H2020 Project called TruBlo¹³. TruBlo is an EU-funded project and part of the NGI (Next Generation Internet) initiative. Participating in TruBlo are six European organisations, three of them currently collaborating also as M-Sec Partners: WLI, ICCS and F6S. The main concept of TruBlo is to fund ideas for reliable content on future blockchains through different open calls. For the TruBlo H2020 project, we are taking advantage of implementations, experience and technical knowledge from M-Sec components such as the IoT Marketplace, Trust and reputation models, Proof-of-validity and proof-of-location tools.



M-Sec is also in ongoing collaboration with its Twin Project called Fed4IoT¹⁴. Fed4IoT offers Virtual Silos as-a-service: isolated and secure IoT environments made of Virtual Things whose data can be accessed through standard IoT Brokers (oneM2M, NGSI, NGSI-LD, etc.). Fed4IoT Cloud of Things offers aspires to enable IoT application developers to simply rent and customize a Virtual Silo instead of deploying physically their IoT infrastructure. The joint collaboration between the two projects relies on connecting the Marketplace into the Fed4IoT platform. Through the M-Sec Marketplace, Virtual Silos can be enriched with available and anonymized data and information acquired by several other networks of sensors and UCs, thus making it less necessary for integrators to rely on new deployments.

5.5 Open Source Approach

Most SW M-Sec components are released as Open Source: just three out of fourteen components are totally proprietary.

The main benefits to go with an open source approach are:

- Open-Source software code is open to everyone, so bugs can be discovered and fixed more quickly because of all the contributors to the software placed on Github.
- It drives innovation and boosts stakeholders community to re-use M-Sec outcomes and to customize them based on their particular needs.
- It contributes to the overall knowledge of society by sharing the source code.

5.6 Sustainability of the M-sec Framework components

This chapter provides detailed descriptions for the sustainability plan, by analysing each component across five different sub-sections, namely:

- Documentation and code access
- Corrective and adaptive maintenance
- Support services
- Resourcing
- Future plans

In addition, for each FG, a brief explanation and a brochure is provided in order to give a better overview of the Features provided and the System Requirements.

¹³ trublo.eu | Distributed Trust

¹⁴ [Project Overview - Fed4IoT](#)





5.6.1 Development and (Security) Designing Tools

The Development & Security Designing Tools FG aims to establish engineering foundations to support the development of secure smart city applications. Key benefits achieved by this FG include:

- Reduction of developers' effort for analysing security requirements.
- Mitigation of risks related to missing typical security threats.
- Mitigation of risks related to application-level vulnerabilities specifically by human errors.

The Development & Security Designing Tools FG in M-Sec provides the following key components:

- Security Analysis Tool (SAT)
- Modal Transition System Analyzer (MTSA)

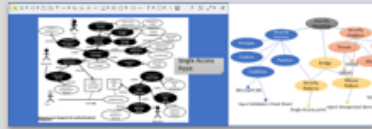
APPLICATION SECURITY

SUPPORT SECURE SMART CITY APPLICATIONS' DEVELOPMENT

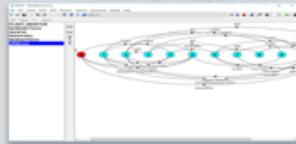
Brief description about the FG "Although smart city platform itself is secured, application-level vulnerabilities make systems insecure. However, ensuring application-level security requires tremendous efforts for developers. The Application Functional Group provides a set of methodologies and tools to support development of secure smart city applications on top of the M-sec platform."

FEATURES

- The *Security Analysis Tool (SAT)* supports security requirement analysis by reusing typical threats and their mitigation approaches stored in a knowledge base.
- The *Modal System Transition Analyzer (MTSA)* supports designing secure smart city applications by synthesizing a correct specification ensured to satisfy application-level security requirements.






Security Analysis Tool



Modal System Transition Analyzer

KEY BENEFITS

-  *reduce engineers' effort for analyzing security requirements*
-  *mitigate risks to miss typical security threats*
-  *mitigate typical risks from human errors in designing the application logic and reduce the wide number of tests performed to verify the security level.*

SYSTEM REQUIREMENTS

- MTSA can run on Java runtime
- SAT is implemented as a plugin of astah* (an UML modeling tool developed by Change Vision, Inc.)

DID YOU KNOW?

What is the unique about the component? What makes it stand out from the competitors?

M-Sec provides a set of cutting-edge tools supporting developers to systematically analyze, design, and implement secure smart city applications.

Figure 51. Development & Security Designing Tools FG Brochure



Table 9. SAT & DMSS Sustainability

| Module: | SAT & DMSS | Owner: | NII |
|---|-----------------------|---------------|------------|
| <p>The Security Analysis Tool (SAT) supports security requirement analysis based on security threat patterns and analysis guidelines stored in security knowledge to specify security requirements. The Security Analysis Tool (SAT) supports the Development method for secure software (DMSS) to specify security requirements based on security threat patterns and analysis guidelines stored in security knowledge.</p> <p>The documentation related to SAT can be found in the deliverable “D4.8 Application Security” available on the M-Sec website (https://www.msecproject.eu/deliverables).</p> <p>The source code and a user manual are available in a public GitHub repository and will be online for at least 12 months after the end of the project.</p> <p>GitHub repository: https://github.com/MSec-H2020/Security_Analysis_Tool</p> | | | |
| Corrective and adaptive maintenance | | | |
| <p>The Security Analysis Tool (SAT) is implemented as a plugin of astah* (a UML modeling tool developed by Change Vision, Inc.). The SAT has been developed and maintained for research purposes.</p> <p>Tasks to be conducted are</p> <ul style="list-style-type: none">• Bug fixes.• Documentation updates.• Improving the methodology of the SAT with the security analysis research. | | | |
| Support Services | | | |
| <p>As NII is an inter-university research institute in Japan, they do not have particular support service. However, the SAT Tool can be used and modified under the APACHE LICENSE 2.0 by any user.</p> | | | |
| Resourcing | | | |
| <p>NII features in a wide range of research activities on information security. This provides additional resources for the improvement of the SAT.</p> | | | |
| Future plans | | | |
| <p>NII will continue to research security analysis and to develop new tools. It may be possible to collaborate with researchers by using the SAT.</p> | | | |





Table 10. MTSA Sustainability

| | | | |
|--|------|---------------|----|
| Module: | MTSA | Owner: | WU |
| Documentation and code access | | | |
| <p>This component is a bridge between MTSA and NodeRED, which supports secure smart city application development. It provides the functionality of translating behaviour specification models synthesized by MTSA to NodeRED programs.</p> <p>A document related to the MTSA-NodeRED Translator is in in Section 3.3 of the deliverable “D4.8 M-Sec application level security – final version”, which is available on the M-Sec website (https://www.msecproject.eu/deliverables).</p> <p>The source code is available in a public GitHub repository.</p> <p>GitHub repository: https://github.com/MSec-H2020/MTSA-NodeRed-Translator</p> | | | |
| Corrective and adaptive maintenance | | | |
| <p>This component is developed and maintained by Waseda University. After this project, it will be used in WU’s research. Its maintenance activities can be guaranteed beyond the proposed 12 months. Tasks to be conducted include:</p> <ul style="list-style-type: none">• Bug fixes.• Documentation update.• Identification of the use of external libraries that are not up to date. | | | |
| Support Services | | | |
| <p>Waseda University will guarantee the maintenance of the MTSA-NodeRED Translator during at least 12 months after the project conclusion, mainly because the module will be re-used in future research and development projects.</p> <p>For the communication of incidents, the reporting tools offered by GitHub will be used. The existing capabilities will be maintained through GitHub issues.</p> | | | |
| Resourcing | | | |
| <p>The Waseda University research team works on different projects that take advantage of this component, and that is why the cost of maintenance or support that may arise can be absorbed by these other initiatives.</p> | | | |
| Future plans | | | |
| <p>The MTSA-NodeRED Translator will be used in a tool chain with MTSA, NodeRED, and SecureSOXFire, which are assets used in smart city application scenarios in Fujisawa city. Waseda University will continue joint work with KEIO and Fujisawa city after the M-Sec project, and will apply this component to other smart city application and refine it through further experience.</p> | | | |



5.6.2 IoT Marketplace FG

The M-Sec IoT Marketplace is a marketplace where smart objects can exchange data through the use of virtual currencies allowing the real-time matching of supply and demand and enabling the creation of liquid markets with profitable business models of the IoT stakeholders.

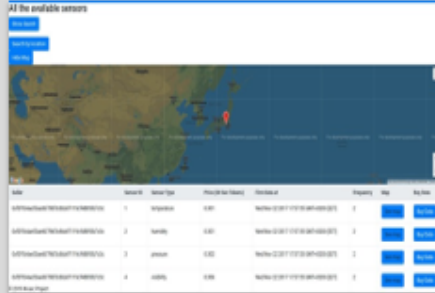
IoT Marketplace

Implementation of a novel marketplace, where smart objects can exchange information and services, through the use of virtual currencies.

Brief description about the FG “The FG implements a platform to assist the exchange of IoT devices data, as well as media, between registered users from all over the world. It is accessible through its web browser and API endpoints and the data exchanged can be distributed on off-chain and on-chain databases.”

FEATURES

- “IoT sensor data and media exchange.”
- “User authentication and anonymity within the app.”
- “Accessible through web app and API clients.”
- “Enhanced Security based on Blockchain and end-to-end encrypted communication.”
- “KYC and Trust & Reputation mechanisms”




| ID | Name | Model | Manufacturer | Location | Property | Age | Value |
|----|-------------|-------|--------------|-------------|----------|-----|-------|
| 1 | Temperature | 1 | Arduino | 10.10.10.10 | 1 | 10 | 10 |
| 2 | Humidity | 2 | Arduino | 10.10.10.10 | 2 | 10 | 10 |
| 3 | Pressure | 3 | Arduino | 10.10.10.10 | 3 | 10 | 10 |
| 4 | Light | 4 | Arduino | 10.10.10.10 | 4 | 10 | 10 |


KEY BENEFITS




“Safely and easily register, sell and purchase IoT device data and media.”



“Support of purchases using M-Sec tokens.”



“User friendly UI with visual aids (map view).”



“End-to-end encrypted communication with the server.”

SYSTEM REQUIREMENTS

- “The IoT Marketplace server runs on NodeJS.”
- “The front-end web client can be accessed from common browsers, while the exposed API responds to JSON requests.”
- “TLS/SSL certificates are obtained from certified well-known providers.”
- Smart Contracts deployed on Blockchain.

DID YOU KNOW?

“M-sec IoT marketplace users can exchange IoT sensor data and media easily, securely and with complete anonymity. It allows the real-time matching of supply and demand enabling the creation of liquid markets with profitable business models of the IoT stakeholders. IoT devices and humans using mobile applications and APIs are able to exchange data and value through the M-Sec blockchain-based implementations.”

Figure 52. IoT MarketPlace FG Brochure





Table 11. IoT Marketplace Sustainability

| | | | |
|--|-----------------|---------------|------|
| Module: | IoT Marketplace | Owner: | ICCS |
| Documentation and code access | | | |
| <p>IoT marketplace users can exchange IoT sensor data and media easily, securely, and with complete anonymity. It allows the real-time matching of supply and demand enabling the creation of liquid markets with profitable business models of the IoT stakeholders. IoT devices and humans using mobile applications and APIs are able to exchange data and value through the M-Sec blockchain-based implementations.</p> <p>The documentation about IoT Marketplace can be found in D4.8 Application Security available on the M-Sec website (https://www.msecproject.eu/deliverables).</p> <p>The code and installation instructions for IoT Marketplace are available in a public GitHub repository https://github.com/MSec-H2020/IoT_Marketplace</p> | | | |
| Corrective and adaptive maintenance | | | |
| <p>The IoT Marketplace is part of the catalogue of components used by ICCS in the development of new solutions and services and it is for this reason that maintenance activities can be guaranteed beyond the proposed 12 months. Tasks to be performed for its maintenance include:</p> <ul style="list-style-type: none">• Analysis and diagnosis of incidents and their causes.• Bug fixes.• Documentation updates.• Monitoring updates of various external libraries. | | | |
| Support Services | | | |
| <p>ICCS will guarantee the maintenance of the IoT Marketplace for at least 12 months after the project conclusion mainly because the module will be available for reuse in other research and development projects as well as for PhD research.</p> <p>For the communication of incidents, the reporting tools offered by GitHub will be used. The existing capabilities will be maintained through GitHub issues. In addition to the various channels available in the project, the following email can be used: hello@msecproject.eu</p> | | | |
| Resourcing | | | |
| <p>The ICCS team works on various projects that take advantage of this component. For this reason, the maintenance and support that may arise can be absorbed by these other initiatives.</p> | | | |
| Future plans | | | |
| <p>ICCS plans to evolve the IoT Marketplace asset and develop it further by incorporating it in its technology assets portfolio of other projects (e.g. H2020 projects like TruBlo, Pledger, etc.).</p> | | | |





5.6.3 Devices Security FG & Cloud Tools

For the Devices Security FG, the following key security components are described:

- Secured components for devices.
- Perimeter defense (Intrusion Detection System).
- Stealth security.
- Security monitoring and visualisation tool.

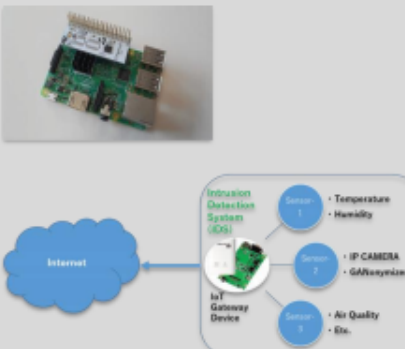
DEVICE SECURITY

APPLY NOVEL HARDWARE AND SOFTWARE SOLUTIONS TO CREATE SECURE MONITORING IoT DEVICES


Even though current smart city platforms themselves are secured, device level vulnerabilities put the whole system at risk. It is a fact that ensuring device-level security requires tremendous efforts for IoT providers. **M-Sec's Device Security Functional Group** provides a set of methodologies and tools to support development of secure smart city IoT devices on top of the M-sec platform.

FEATURES


- **Secured IoT Device** A hardware based solution to provide an embedded security layer to diverse-purpose IoT devices.
- **Intrusion Detection System (IDS)** A software-based solution to provide a secure IoT mobile sensing platform by monitoring and preventing cyber attacks




KEY BENEFITS




Secure encryption and decryption of data generated by different sensors



Introduction of secure boot mechanisms



Monitoring and reporting, along with the option for blocking malicious traffic matching known signatures



Configured rules to protect IoT devices from a potential attack

SYSTEM REQUIREMENTS

- HW solution apt for STM32-L4 based devices
- HW solution apt for Raspberry PI-based devices
- SW solution based on Open Source Software (OSS) not needing any licensing.

DID YOU KNOW?

The **Secured IoT Device** hardware and software solution provides IoT devices with mechanisms to assure they are properly protected both at the time of booting and the moment they proceed to send data generated by their sensors, avoiding external interferences and malicious tweaks.

The lightweight **Intrusion Detection System** software has been customized with OS hardening to reduce attack surface, secured communication using Transport Layer Security (TLS), and signature patterns obtained from the testing and analysis in the IoT honeypot, besides other well-known up-to-date attack signature patterns provided by open source resources

Figure 53. Device Security FG Brochure



Table 12. Secured Components for Devices Sustainability

| | | | |
|--|--------------------------------|---------------|-----|
| Module: | Secured Components for Devices | Owner: | CEA |
| Documentation and code access | | | |
| <p>The “Secured Components for Devices” asset is a collection of several components in order to elevate the security level of an existing or upcoming device. Its principle is to integrate a hardware component compliant to the TPM2 specification from the TCG. On top of this component, we have built specific software parts to mitigate some cybersecurity risks. The specific parts are optimized for embedded platforms, which makes this solution novel.</p> <p>A collection of patches and configuration primitives completes this asset. They depend strongly on the hardware destination as well as its operating systems and requires customization.</p> | | | |
| Corrective and adaptive maintenance | | | |
| <p>Patches for third party components have been submitted, or are in the process of submission, in order to use these components maintenance workflow.</p> | | | |
| Support Services | | | |
| <p>CEA have put in place a gitlab instance https://gitlab.msecproject.eu/ in order to grant an access to both public and restricted code. An issue tracker is available in this gitlab instance to submit and track support requests.</p> | | | |
| Resourcing | | | |
| <p>Maintenance is expected to be almost costless as access to the code is granted to partners. Thus, as new features are being implemented in the scope of other projects, further releases may solve reported bugs.</p> | | | |
| Future plans | | | |
| <p>The development of this asset is continued within CEA in order to reach higher security level at the cost of stronger hardware requirements in particular trust zone.</p> | | | |

Table 13. Intrusion Detection System Sustainability

| | | | |
|---|----------------------------|---------------|-----|
| Module: | Intrusion Detection System | Owner: | YNU |
| Documentation and code access | | | |
| <p>Internet connectivity exposes IoT devices to potential threats from bad actors (cyber-criminals) with malicious intent. This component is a lightweight Intrusion Detection System (IDS) customized for providing detection and prevention capabilities to the perimeter defense of M-Sec UC3 IoT devices layer.</p> | | | |





| |
|---|
| <p>A document related to this security option is available in Section 2.2 of the deliverable “D4.2: M-Sec IoT security layer – final version”, which is available on the M-Sec website (https://www.msecproject.eu/deliverables).</p> <p>An up-to-date source code is maintained by OISF on github and is available on Suricata. A copy of the customized M-Sec solution is available on the GitHub repository: https://github.com/MSec-H2020/Intrusion_Detection-System</p> |
| Corrective and adaptive maintenance |
| <p>This component is based on <u>Suricata</u> Open Source Software (OSS) under the <u>GNU General Public License v2</u> or later. YNU can provide guidance on its use with M-Sec UC3 IoT devices or similar for 12 months after the completion of the project.</p> |
| Support Services |
| <p>YNU shall provide guidance on its installation and use with M-Sec UC3 IoT devices or similar for 12 months after the completion of the project.</p> |
| Resourcing |
| <p>YNU research team works on various projects, so resolving any technical issues in using this feature with M-Sec UC3 IoT devices or similar can be absorbed via an ongoing project or internal resources.</p> |
| Future plans |
| <p>The IDS security option is designed as part of the perimeter defense of M-Sec UC3 IoT devices for detecting and preventing known security threats to M-Sec IoT layer being deployed in Fujisawa city. YNU will continue to work with KEIO and Fujisawa city after the completion of M-Sec project, and can engage in future projects for applying advance security options leveraging its expertise and experiences in the information security environment.</p> |

Table 14. Monitoring & Visualisation Tool Sustainability

| | | | |
|---|---------------------------------|---------------|-----|
| Module: | Monitoring & Visualisation Tool | Owner: | YNU |
| Documentation and code access | | | |
| <p>This component is part of the perimeter defense developed for detecting and monitoring possible security threats to the M-Sec UC3 IoT layer. The tool is based on the Amazon Elastic-Search Service (AESS) for collecting and examining the log activity from embedded agents in the IoT devices.</p> <p>A document related to the monitoring & visualization tool is available in Section 2.2 of the deliverable “D4.2: M-Sec IoT security layer – final version”, which is available on the M-Sec website (https://www.msecproject.eu/deliverables).</p> | | | |





| |
|--|
| As this was developed as a service using Amazon Web Services (AWS), so a guide is available on the GitHub repository: https://github.com/MSec-H2020/Monitoring_and_Visualisation_Tool |
| Corrective and adaptive maintenance |
| This component was developed in the cloud using AESS as a service under the Elastic/Apache License. Therefore, AWS controls the source code or its maintenance and availability, and should be referred to for bugs, guides, and documentation updates. YNU can provide guidance on its use with M-Sec UC3 IoT devices or similar for 12 months after the completion of the project. |
| Support Services |
| This tool runs on the cloud service that is managed by the amazon web services. Therefore, YNU can only provide guidance on how-to-use with M-Sec UC3 IoT devices or similar for 12 months after the completion of the project. |
| Resourcing |
| YNU research team works on various projects, so resolving any technical issues in using this feature with M-Sec UC3 IoT devices or similar can be absorbed via an ongoing project or internal resources. |
| Future plans |
| The visualization tool is designed as part of the perimeter security of M-Sec UC3 IoT devices for detecting and monitoring security of M-Sec IoT layer being deployed in Fujisawa city. YNU will continue to work with KEIO and Fujisawa city after the completion of M-Sec project, and can engage in future projects for applying advance security options leveraging its expertise and experiences in the information security environment. |

Table 15. Stealth Security Sustainability

| | | | |
|---|------------------|---------------|-----|
| Module: | Stealth Security | Owner: | YNU |
| Documentation and code access | | | |
| <p>This security option helps in addressing the unknown attacks and zero day threats. As the attackers need to know which ports are open and what service is being provided for conducting an attack, this stealth security feature further strengthens the security by hiding the ports from unauthorized attempts/scans for obtaining intelligence. Another advantage of this security feature is that it makes the IoT device consume less power than it would have consumed without it.</p> <p>Besides a published paper (doi: 10.2197/ipsjjip.29.572), a document related to the stealth security feature is also available in Section 2.2 of the deliverable “D4.2: M-Sec IoT security layer – final version”, which is available on the M-Sec website (https://www.msecproject.eu/deliverables).</p> <p>The source code is available on the GitHub repository: https://github.com/MSec-H2020/Stealth_Security</p> | | | |





| |
|---|
| Corrective and adaptive maintenance |
| This component is based on Open Source Software (OSS) under MIT License . YNU can provide guidance on its use with M-Sec UC3 IoT devices or similar for 12 months after the completion of the project. |
| Support Services |
| YNU shall provide guidance on its installation and use with M-Sec UC3 IoT devices or similar for 12 months after the completion of the project. |
| Resourcing |
| YNU research team works on various projects, so resolving any technical issues in using this feature with M-Sec UC3 IoT devices or similar can be absorbed via an ongoing project or internal resources. |
| Future plans |
| The stealth security feature (port knocking) designed for use with M-Sec UC3 IoT devices is part of security options for securing M-Sec IoT layer being deployed in Fujisawa city. YNU will continue to work with KEIO and Fujisawa city after the completion of M-Sec project, and can engage in future projects for applying advance security options leveraging its expertise and experiences in the information security environment. |



5.6.4 Privacy Management FG

The privacy management functional group aims to address the requirements from GDPR & APPI standards for the privacy of personal identifiable information (PII) by anonymizing any such identifiable information from the video camera images being captured by the IP cameras mounted on smartphone applications or IoT devices.

This FG is composed by only one component called GANonymizer. The GANonymizer uses deep learning-based object detection techniques to automatically detect objects related to personal information.

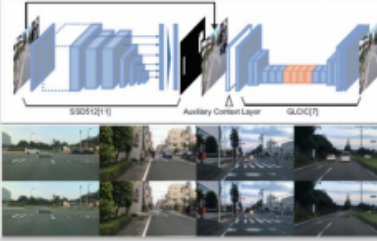
PRIVACY MANAGEMENT

PRIVACY PROTECTED MONITORING AND SENSING


In situations where video data is used in various IoT Smart City applications, personal information is a problem. As one of the solutions, M-Sec's Privacy Management Functional Group provides "GANonymizer" that automatically removes objects with privacy risk from image data based on advanced deep learning image processing technology.

FEATURES

"GANonymizer" consists of two parts of neural networks. In order to detect the target objects from the input image, which might violate the privacy, we adopt the deep neural networks: Single Shot Multibox Detector (SSD). And in order to generating more natural image, we adopt Globally and Locally Consistent Image Completion (GLCIC) which is one of the most successful models in image completion.



KEY BENEFITS



From the viewpoint of privacy protection, it automatically detects and deletes risky targets.



It can process not only still images but also moving images.



The deleted part is automatically repaired with a natural background.



An API is provided so that it can be incorporated in various situations where privacy protection is

SYSTEM REQUIREMENTS

- It is a completely SW solution and can be provided as OSS in the future.
- Especially when performing real-time processing on video, it is necessary to check the processing capacity of the cloud / edge computing environment.

DID YOU KNOW?

Anonymization for privacy protection in image data can be done by methods such as mosaic video, but using "GANonymizer" not only erases the object automatically, but also creates a natural background automatically as if the object did not exist.

Figure 54. Privacy Management FG Brochure





Table 16. GANonymizer Sustainability

| | | | |
|--|-------------|---------------|------|
| Module: | GANonymizer | Owner: | KEIO |
| Documentation and code access | | | |
| <p>KEIO will create a web page for this software, probably on https://www.jn.sfc.keio.ac.jp/ganonymizer, on which KEIO will provide newer versions of the software, documents, libraries, and sample applications. The page will be linked to the github of the M-Sec Project.</p> <p>The documentation about GANonymizer can be found in D4.4 M-Sec cloud and data level security available on the M-Sec website (https://www.msecproject.eu/deliverables).</p> | | | |
| Corrective and adaptive maintenance | | | |
| <p>GANonymizer is an automatic erasure technology for privacy data that utilizes deep learning that Keio University has been working on, and we are considering expanding it to cities starting from Fujisawa City. KEIO will undertake the following:</p> <ul style="list-style-type: none">• Analysis and diagnosis of incidents and their causes.• Bug fixes.• Documentation update.• Update of various external libraries. | | | |
| Support Services | | | |
| <p>KEIO will create (1) web page to which newer versions, documents, and libraries will be uploaded, (2) an e-mail account <jn-msec@sfc.keio.ac.jp> to receive bug reports, and (3) a team of developers for future versions of this software.</p> | | | |
| Resourcing | | | |
| <p>KEIO will use internal resources mainly, but leverage funds from 3rd parties too.</p> | | | |
| Future plans | | | |
| <p>KEIO will use Secure GANonymizer for other Smart-city related projects. One of them is ongoing with a local bus company, named Kanagawa Chuo Kotsu, whose goal is to visualize people density in busses. In this project, KEIO will leverage camera images inside a bus to detect the density. The calculation, in some cases, may be conducted at the server-side, so the images have to be anonymized using this software.</p> | | | |



5.6.5 Secure City Data Access

The goal of the Secure City Data Access Functional Group is to act as a bridge between IoT devices and applications. In the manner of IoT platforms, this functional group (middleware layer) includes two parts:

- Southbound access which deals with devices related functional groups. It handles various IoT protocols and standards and compiles data in a common model.
- Northbound access which deals with the storage FG. It provides access to data using different web services and format given the affinity of each application vendor.

The FG is composed mainly of two components:

- Keio SOXFire can provide practical distributed and federated infrastructure for IoT sensor data sharing among various users/organizations in a way that is scalable, extensible, easy to use, and secure with preserving privacy.
- Eclipse Sensinact Platform & Studio implements the basic blocks for connectivity, service abstraction, device management, virtualization, and remote access. The sensiNact Gateway allows interconnection of different networks to achieve secured access and communication with embedded devices.

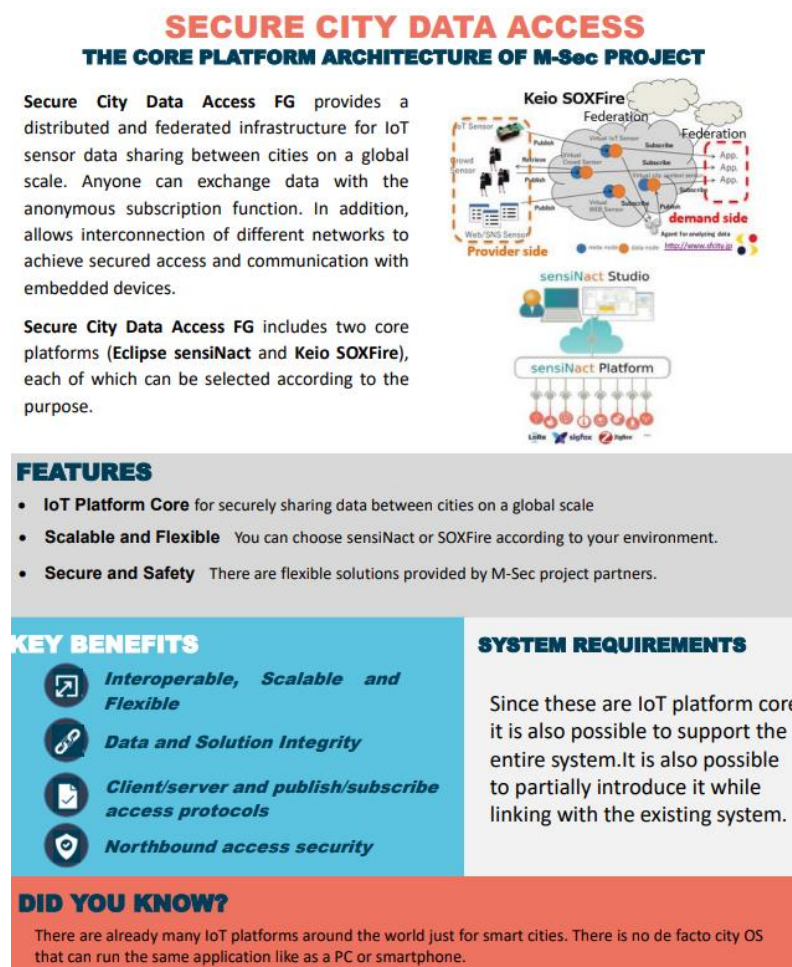


Figure 55. Secure City Data Access FG Brochure





Table 17. Eclipse Sensinact Studio & Platform Sustainability

| | | | |
|---|----------------------------|---------------|-----|
| Module: | Eclipse Sensinact Platform | Owner: | CEA |
| Documentation and code access | | | |
| <p>SensiNact code and documentation is open source and accessible from Eclipse's website.</p> <p>https://projects.eclipse.org/projects/technology.sensinact</p> <p>https://projects.eclipse.org/projects/technology.sensinact/developer</p> | | | |
| Corrective and adaptive maintenance | | | |
| <p>Eclipse sensiNact is creating a community of developers to develop additional functionalities and provide maintenance and support to existing code. Kentyou, spin-off from CEA, will be in charge of providing the necessary support for the adapters of the Eclipse sensiNact.</p> <p>Eclipse sensiNact has a bug tracking and incidence system based on Bugzilla.</p> | | | |
| Support Services | | | |
| <p>Part of Kentyou's strategy is to create a community of developers and users of Eclipse sensiNact. The project is attracting committers from outside of CEA and Kentyou and will be included as official committers to the project.</p> <p>Eclipse sensiNact has a bug tracking and incidence system based on Bugzilla.</p> | | | |
| Resourcing | | | |
| <p>The maintenance and support will be financed both by internal resources to Kentyou, as well as external resources such as public funding for open source solutions, including application oriented Horizon Europe projects.</p> | | | |
| Future plans | | | |
| <p>The startup Kentyou is now transferring the Eclipse sensiNact to the industry. Based on the open core model, Kentyou is starting to commercialise value-added services and products around sensiNact's the open core. It will be increasingly improved with additional innovation projects and industrial partnerships.</p> | | | |





Table 18. Secure SOXfire Sustainability

| | | | |
|---|----------------|---------------|------|
| Module: | Secure SOXfire | Owner: | KEIO |
| Documentation and code access | | | |
| <p>KEIO will create a web page for this software, probably on https://www.jn.sfc.keio.ac.jp/soxfire, on which KEIO will provide newer versions of the software, documents, libraries, and sample applications. The page will be linked to the github of the M-Sec Project.</p> <p>The documentation about Keio SOXFire can be found in D4.4 M-Sec cloud and data level security available on the M-Sec website (https://www.msecproject.eu/deliverables).</p> | | | |
| Corrective and adaptive maintenance | | | |
| <p>Secure SOXFire is based on the smart city platform that Keio University has been working with Fujisawa City for many years. KEIO will continue to updating the tool based on future efforts:</p> <ul style="list-style-type: none">• Analysis and diagnosis of incidents and their causes.• Bug fixes.• Documentation updates.• Monitoring updates of various external libraries. | | | |
| Support Services | | | |
| <p>KEIO will create (1) web page to which newer versions, documents, and libraries will be uploaded, (2) an e-mail account <jn-msec@sfc.keio.ac.jp> to receive bug reports, and (3) a team of developers for future versions of this software.</p> | | | |
| Resourcing | | | |
| <p>KEIO will use internal resources mainly, but leverage funds from 3rd parties too.</p> | | | |
| Future plans | | | |
| <p>KEIO will use Secure SOXFire for other Smart-city related projects. One of them is ongoing with a local bus company , named Kanagawa Chuo Kotsu, whose goal is to visualize CO₂ density in busses. Another project (though still at planning phase) is related to building Smart trash boxes for citizens to separate the garbage into categories so that plastic materials can be fully recycled. Secure SOXFire will be used in both of these projects to collect trustworthy sensor data.</p> | | | |

5.6.6 Secured & Trusted Storage FG

As the name implies, this FG is focused on providing tools and mechanisms that enhance the security of the M-Sec overall solution at the Storage level. To achieve that, M-Sec exploits both a blockchain-focused





approach and an encrypted database one. By storing and encrypting the main core of the data off-chain on the Cloud and storing the corresponding metadata and interactions-related data on-chain, M-Sec couples the benefits of both the P2P and Cloud solution.

The Secured and Trusted Storage FG consists of three main components: the Crypto Companion Database, the Quorum Blockchain/Blockchain middleware, and the Trust & Reputation Management.

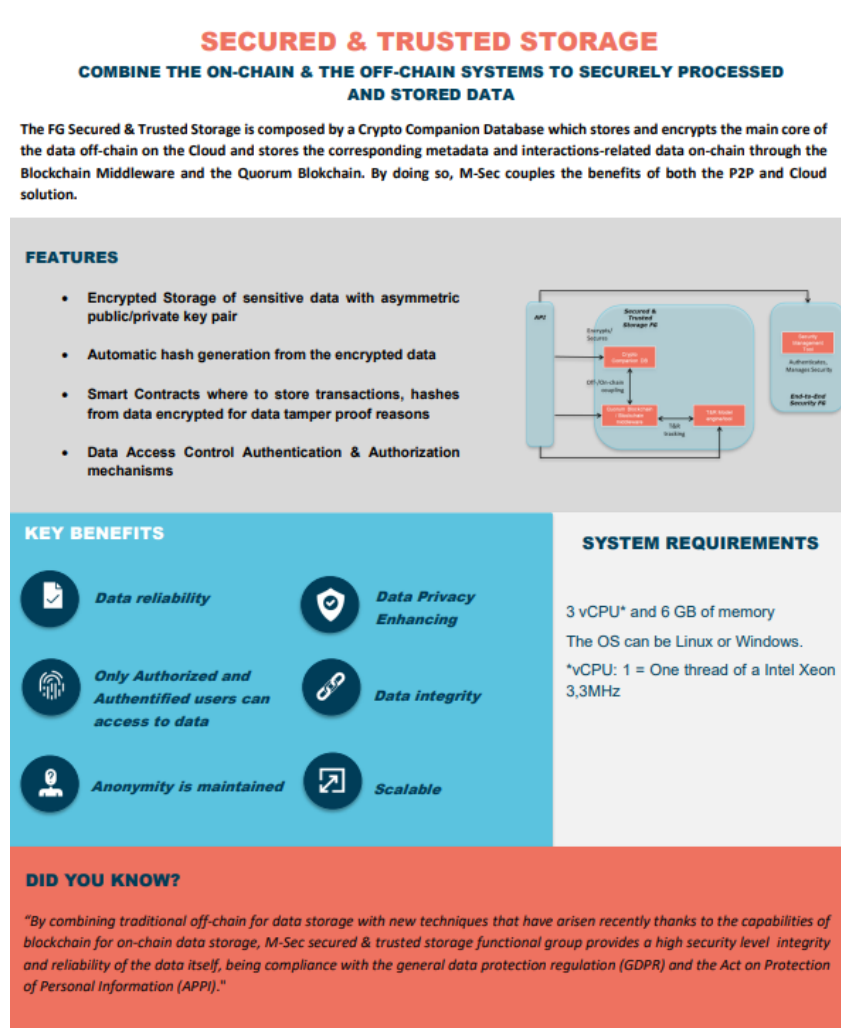


Figure 56. Secured & Trusted Storage FG Brochure

Table 19. Crypto Companion DB Sustainability

| | | | |
|--|---------------------|---------------|-----|
| Module: | Crypto Companion DB | Owner: | WLI |
| Documentation and code access | | | |
| This component provides an API to encrypt/decrypt data with an asymmetric public/private key pair. The data can only be accessed by the owner, who will have to be authenticated, and the authorized operators allowed by the owner. | | | |



The documentation related to the Crypto Companion DB can be found in the deliverable “D4.6 P2P Level Security and M-Sec Blockchain” available on the M-Sec website (<https://www.msecproject.eu/deliverables>). The documentation can be found in section 2 “Secured and Trusted Storage FG” with the name Crypto Companion Database inside the document. The source code is available in a public GitHub repository and it will be online for at least 12 months after the end of the project.

GitHub repository: https://github.com/MSec-H2020/Crypto_Companion_DB

Corrective and adaptive maintenance

The Crypto Companion DB is part of the catalogue of components used by Worldline in the development of new solutions or services and it is for this reason that maintenance activities can be guaranteed beyond the proposed 12 months. Tasks to be conducted are:

- Analysis and diagnosis of incidents and their causes.
- Bug fixes.
- Documentation update.
- Identification of the use of external libraries that are not up to date.
- Tasks related to updating and maintaining documentation, reviewing and improving processes.

Support Services

Worldline will guarantee the maintenance of the CCDB during at least 12 months after the project conclusion, mainly because the module will be available for re-use in other development projects for shorter times to market and for future research projects or company products.

For the communication of incidents, the reporting tools offered by GitHub will be used. The existing capabilities will be maintained through GitHub issues. In addition to the various channels available in the project, the following email can be used: hello@msecproject.eu

Resourcing

The Worldline R&D team works on different projects that take advantage of this component, and that is why the cost of maintenance or support that may arise can be absorbed by these other initiatives.

Additionally, Worldline is using this asset as part of solutions derived from internal innovation projects financed by the company itself and external projects financed by clients. This provides additional resources for the sustainability of the component.

Future plans

The Crypto Companion DB is integrated in Use Case 2 Home Monitoring Security for Ageing People, where Worldline is the owner of the solution “Connected Care”. As a value added to guarantee data integrity and protection, the value proposition of Use Case 2 contemplates the security offered by this component. Furthermore, Crypto Companion DB works with the component Quorum Blockchain to provide additional security by generating a hash of the encrypted data to be stored in the blockchain for data tamper proof





reasons. Worldline has identified Blockchain technology as one of the most strategic ones for their future value propositions to their customers.

Table 20. Quorum Blockchain / Blockchain Middleware Sustainability

| Module: | Quorum Blockchain / Blockchain Middleware | Owner: | ICCS |
|---|---|--------|------|
| Documentation and code access | | | |
| <p>The main focus of this Component is to implement the M-Sec blockchain framework, and to facilitate the convergence of IoT security with blockchains in order to support an innovative smart city platform. ICCS used Ethereum-based blockchains as the basic foundation of M-Sec blockchain, as they enables not only the exchange of value (M-Sec tokens), but also the enforcement of smart contracts, which provide an additional feature for the implementation and validation of the selected M-Sec use cases.</p> <p>The documentation about Quorum Blockchain / Blockchain Middleware can be found in D4.6 “P2P level security and M-Sec blockchains” available on the M-Sec website (https://www.msecproject.eu/deliverables).</p> <p>The code and installation instructions for Quorum Blockchain / Blockchain Middleware are available in our public GitHub repository:</p> <p>https://github.com/MSec-H2020/Quorum_Blockchain_and_Blockchain_Middleware</p> | | | |
| Corrective and adaptive maintenance | | | |
| <p>The Quorum Blockchain / Blockchain Middleware can is part of the catalogue of components used by ICCS in the development of new solutions and services and it is for this reason that maintenance activities can be guaranteed beyond the proposed 12 months. Tasks to be performed for its maintenance include:</p> <ul style="list-style-type: none">• Analysis and diagnosis of incidents and their causes.• Bug fixes.• Documentation update.• Monitoring updates of various external libraries. | | | |
| Support Services | | | |
| <p>ICCS will guarantee the maintenance of the Quorum Blockchain / Blockchain Middleware during at least 12 months after the project conclusion, mainly because the module will be available to be re-used in other research and development projects as well as for PhD research.</p> <p>For the communication of incidents, the reporting tools offered by GitHub will be used. The existing capabilities will be maintained through GitHub issues. In addition to the various channels available in the project, the following email can be used: hello@msecproject.eu</p> | | | |





| |
|---|
| Resourcing |
| The ICCS team works on various projects that take advantage of this component. For this reason, the maintenance and support that may arise can be absorbed by these other initiatives (e.g. internal or national research funds, EC research grants, etc.). |
| Future plans |
| ICCS plans to evolve the Quorum Blockchain / Blockchain Middleware asset and develop it further by incorporating it in its technology assets portfolio of other projects (e.g. H2020 projects like TruBlo, Pledger, etc.). |

Table 21. T&R Model Engine/Tool Sustainability

| | | | |
|--|-----------------------|---------------|------|
| Module: | T&R Model Engine/Tool | Owner: | ICCS |
| Documentation and code access | | | |
| <p>T&R engine acts on top of the Blockchain Middleware Services and the IoT Marketplace. Such an engine would enhance the security mechanisms of M-Sec and make it possible to evaluate the actual content being shared through the Blockchain and the Marketplace, thus ensuring the trustworthiness of the several actors participating in the exchange or sharing of information, data and services.</p> <p>The code for T&R Model Engine/Tool is available in a public GitHub repository: https://github.com/MSec-H2020/Secured-and-Trusted-Storage-FG</p> <p>The documentation about T&R Model Engine/Tool can be found in D4.6 “P2P level security and M-Sec blockchains” available on the M-Sec website (https://www.msecproject.eu/deliverables).</p> | | | |
| Corrective and adaptive maintenance | | | |
| <p>The T&R Model Engine can is part of the catalogue of components used by ICCS in the development of new solutions and services and it is for this reason that maintenance activities can be guaranteed beyond the proposed 12 months. Tasks to be performed for its maintenance include:</p> <ul style="list-style-type: none">• Analysis and diagnosis of incidents and their causes.• Bug fixes.• Documentation update.• Monitoring updates of various external libraries. | | | |
| Support Services | | | |
| <p>ICCS will guarantee the maintenance of the T&R Model Engine during at least 12 months after the project conclusion mainly because the module will be available to be re-used in other research and development projects as well as for PhD research.</p> | | | |



For the communication of incidents, the reporting tools offered by GitHub will be used. The existing capabilities will be maintained through GitHub issues. In addition to the various channels available in the project, the following email can be used: hello@msecproject.eu

Resourcing

The ICCS team works on various projects that take advantage of this component. For this reason the maintenance and support that may arise can be absorbed by these other initiatives (e.g. internal or national research funds, EC research grants etc.).

Future plans

ICCS plans to evolve the T&R Model Engine asset and develop it further by incorporating it in its technology assets portfolio of other projects. Moreover, as the specific research topics is of high importance, PhD research will be further conducted by the ICCS research personnel through internal research procedures.





5.6.7 End-to-End Security FG

The end-to-end security functional group aims to provide a global security backend for mixed OT/IT large infrastructures. It is composed by a single component tool called Security Management that provides all-in-one security functions for large-scale IoT infrastructures such as a Public Key Infrastructure for certificates, a directory module for accounting, and an identity federation module for user management.

End to end Security Management

Provide security mechanism to secure data at various points on complex IoT ecosystems

In complex and heterogeneous IoT infrastructure, **End-to-end security functional group** provides a fully interoperable security backend that enables **authentication** of parties, **encryption** of data, **attestation** of devices and **anonymization** of data sources. It helps to enable cyber resilience to provided escalated reactions upon various situations.

FEATURES

- **Identity federation** to benefit interoperable authentication using OAuth2, OpenID and regular directory services such as LDAP
- **Asymmetric encryption** support with an embedded Public Key Infrastructure bound to identities
- **Remote attestation** of IoT devices based on Trusted Computing Group (TCG) specifications and component such as Trusted Platform Module (TPM)
- **Anonymization** support with Direct Anonymous Attestation (ECDA) to comply with privacy matters

KEY BENEFITS

Easy to integrate

Compliant with TCG's specifications

All-in-one security management

High scalability with clustering

Remediation examples included

Collaborative

SYSTEM REQUIREMENTS

For IoT devices:

- an hardware, firmware or software TPM2 compliant device
- measured boot
- IMA and EVL module in Linux Kernel

For Edge/Network:

- Radius or LDAP authentication capabilities

For applications:

SASL, OAuth2 and OpenID

DID YOU KNOW?

Misconfiguration and misalignment of security standard and procedure in complex system makes room for vulnerabilities. Our End-to-end solution provides a common backend to make sure various entity can benefit from a single interoperable security platform. It provides secured framework for devices, edge components, application's backend and frontend using well-known, tested and trustful components such as OpenSSL, TPM2, LDAP and PKCS standards.

End-to-end Security Managers provides unique features for cyber-resilience with automated remediation upon incident. The whole system is actively monitored and audited making security manageable during its lifecycle.

Figure 57. End to End Security FG Brochure





Table 22. Security Management Tool Sustainability

| | | | |
|---|--------------------------|---------------|-----|
| Module: | Security Management Tool | Owner: | CEA |
| Documentation and code access | | | |
| <p>The security manager is an integrated collection of security tools to provide an interoperable security backend for large scale IoT infrastructures. It contains:</p> <ul style="list-style-type: none">• A public private key infrastructure.• A user identity federation module.• An accounting and authorization directory.• A remote attestation module (both authenticated and anonymous methods).• A collection of application to enrol, revoke and manage devices. <p>It is provided by CEA on a private gitlab instance with an access restricted to M-Sec partners.</p> | | | |
| Corrective and adaptive maintenance | | | |
| CEA ensures maintenance through the gitlab instance by using the issue tracker feature. | | | |
| Support Services | | | |
| CEA proposes to use the gitlab instance for support requests. | | | |
| Resourcing | | | |
| The gitlab instance as well as the security manager live instance are self-hosted. CEA will maintain this hosting and operation for at least 12 months after the project ends. | | | |
| Future plans | | | |
| Ongoing discussion within CEA is in progress to evaluate a possible open source release of this tool. | | | |



5.7 Communication Tools

5.7.1 Website

The website of the project is a key resource for the public and stakeholders to view the project results and get in touch with the project partners.

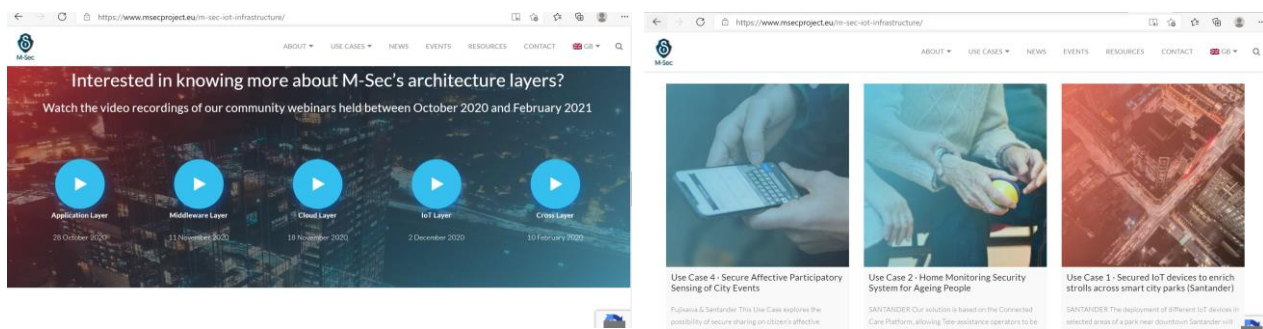


Figure 58. The M-Sec Website

Below are the actions we take to support the sustainability of the project:

- The project website will be maintained and kept available until the end of September 2022, 12 months from the end of the project, so as to enable contact to the project by interested researchers, start-ups or other groups.
- Contact email will be read by two project members. The contact address will be active for at least 12 months after the project conclusion. Any mail to hello@msecproject.eu will be forwarded to two project members (Keiko Doguchi, NTTE, and Vanessa Clemente, WLI).

5.7.2 Consortium internal communication and collaboration

The tools that have been used during the project to keep the internal communications and collaboration will remain available to the consortium for a minimum of 12 months after the end of the project, including in particular:

- Mailing list, based on a Worldline corporate tool.
- Internal site and repository, based on Confluence.
- M-Sec channel, based on Slack.
- Conferencing system, based on Webex.
- M-Sec account on GitHub and Gitlab as source code repository.

Keeping all these tools available ensures the communication and collaboration among M-Sec partners beyond the end of the execution period of the project.





5.8 Contacts and Resources

5.8.1 Contacts

Any request or question related to the project can be addressed to hello@msecproject.eu, managed by the project coordinators (WLI & NTTE) and the communication and dissemination manager (F6S). The managers will handle all requests on a first level or redirect them to the corresponding partners.

- Project coordinator: Vanessa Clemente, Worldline & Keiko Doguchi, NTTE
- Technical coordinator: Antonis Litke, ICCS/NTUA & Jin Nakasawa, KEIO
- Dissemination and Communication Manager: Nadine Teles, F6S
- Exploitation manager: Tomás García, WLI
- UC's Owners:
 - UC1 : Alberto Puras, TST
 - UC2 : Vanessa Clemente, WLI
 - UC3 : Jin Nakazawa, KEIO
 - UC4 : Jin Nakazawa, KEIO
 - UC5 : Keiko Doguchi, NTTE

5.8.2 Resources

5.8.2.1 Information and Documentation

General information about the project can be found on the M-Sec project website <https://www.msecproject.eu/>

The website is updated towards the end of the project to:

- Indicate that the project itself has finished.
- Provide a clear overview and information as to the specific outcomes of the project.

This way we want to further ensure that the project results can be re-used by the community.

All documents generated during the project (whitepaper, scientific papers, and project deliverables) can be found here: <https://www.msecproject.eu/resources/>

5.8.2.2 Software and Tools

Throughout the project, several software modules and tools have been developed. The source code in most cases has been released as open source. Section 2.2 contains an overview of the components from the perspective of their necessity. Following there is a table with an overview of their owners and code repositories:





Table 23. M-Sec Components Repository

| FG | Component | Owner | Code of the Repository |
|--|--|-------|--|
| Development and (Security) Designing Tools | Security Analysis Tool & Development Method for a secure service | NII | https://github.com/MSec-H2020/Secure_Analysis_Tool |
| | Modal Transition System Analyser | WU | https://github.com/MSec-H2020/MTSA-NodeRed-Translator |
| | Eclipse Sensinact Studio | CEA | https://projects.eclipse.org/projects/technology.sensinact/developer |
| Cloud Tools FG | Monitoring and Visualisation Tool | YNU | https://github.com/MSec-H2020/Monitoring_and_Visualisation_Tool |
| Devices FG | Stealth Security | YNU | https://github.com/MSec-H2020/Stealth_Security |
| | Secured Component for Devices | CEA | CEA private GitLab instance. Access restricted to M-Sec partners. https://gitlab.msecproject.eu/ |
| | Intrusion Detection System | YNU | https://github.com/MSec-H2020/Intrusion_Detection-System |
| Privacy Management FG | GANonymizer | KEIO | https://github.com/MSec-H2020/GANonymizer |
| Secure City Data Access | Eclipse Sensinact Platform | CEA | https://projects.eclipse.org/projects/technology.sensinact/developer |
| | Secure SoxFire | KEIO | https://github.com/MSec-H2020/Secure_SOXFire https://github.com/MSec-H2020/SOXStore-Server |
| Secured & Trusted Storage FG | Quorum Blockchain /Blockchain Middleware | ICCS | https://github.com/MSec-H2020/Quorum_Blockchain_and_Blockchain_Middleware |
| | Crypto Companion Database | WLI | https://github.com/MSec-H2020/Crypto_Companion_DB |
| IoT Marketplace FG | IoT Marketplace | ICCS | https://github.com/MSec-H2020/IoT_Marketplace |





End-to-End
Security FG

Security Management Tool

CEA

CEA private GitLab instance. Access
restricted to M-Sec partners.
<https://gitlab.msecproject.eu/>





6. Marketing Strategy

M-Sec continued to follow the Marketing Plan as described in [Deliverable D5.7 Market Analysis and Exploitation – 2nd year](#) (June 2020), i.e., Funnel Phases approach – Awareness, Evaluation, Conversion and Delight – and tried to align the stages of the project’s development with its dissemination and communication activities. In essence, it tried to transform project results (outcomes during project implementation) in impact (outcomes of actions after the project ends).

Overall, the dissemination and communication activities aimed to create visibility and promote the exploitation of the concept and achievements of the M-Sec platform by establishing effective communication channels and appropriate liaisons with all relevant stakeholders.

6.1 Awareness phase

During the awareness phase, it was assumed that potential stakeholders were not aware of neither the consortium nor the solutions provided, and therefore the main goal was to educate potential clients in the challenges they were facing and on potential solutions. This phase corresponded to the first two years (between July 2018 and August 2020) of the project and was part of the dissemination and communication strategy of M-Sec as described in [Deliverable 5.1 Project Website](#) (September 2018) [Deliverable 5.2 Initial Dissemination Plan](#) (December 2018) and [Deliverable 5.9 Community Building Plan](#) (June 2019).

The project tried to interact with the main target audiences (general public, including industry and SMEs, research community, standards and regulation bodies, city field trial stakeholders/community, including citizens and startups and EU-Japan initiatives and policymakers) to collect their needs and present the goals and the M-Sec framework through a robust and informative [website](#) in English and Japanese containing relevant information on the consortium, the project, the Use Cases, Deliverables, main events and other initiatives, among others, with shareable blog posts and a Press kit. It also promoted M-Sec through regular social media posts in Twitter and LinkedIn, and active participation by consortium members in external events and meetings, namely through the close engagement with standardization bodies, and through awareness Webinars on project and Use Cases overview.

The evaluation of the effectiveness of the tools implemented was assessed within the dissemination and communication KPIs of the project and an overview of the main tasks and activities and overall impact can be found in [Deliverable 5.3 Dissemination Activities Report – first year report](#) (June 2019) and [Deliverable 5.4 Dissemination Activities Report – second year report](#) (June 2020).

6.2 Evaluation phase

The evaluation phase corresponded to the first half of the project’s third year (between September 2020 and February 2021). In this phase, it was assumed that potential clients knew they had a problem and were aware of our solution. Therefore, the focus of the dissemination and communication activities was on building trust with the target audiences and create channels for closer interaction, so that they would decide that the M-Sec framework was the solution, among multiple options available, for their challenges.

Essentially, the project focused on building confidence across the ecosystem as the Use Case pilots kicked-off and involved representatives of the previously identified target audiences in a series of activities with the main





goal of demonstrating how the M-Sec framework was used in 5 use case scenarios. During this period, M-Sec delivered, among others, a series of Webinars focused on the layers of the M-Sec architecture – exemplifying the needs, the solutions, and potential applications through the use cases -, closely engaging relevant stakeholders, and presented the initial results in several external events and meetings. These Webinars were the basis for several blog posts, shared in the project’s website and other relevant online communities in which M-Sec took part (e.g., EU Blockchain Observatory and Forum, StandICT.eu European Observatory for ICT Standardisation¹⁵, Cyberwatching.eu¹⁶, etc.). A [Slack channel](#) was also created, apart from the F6S IoT Group, which continued to be regularly updated with the project’s main achievements, to further engage relevant stakeholders and provide a direct channel between consortium members and potential clients or partners.

A [white paper](#) documenting the challenges and how they could be solved using the M-Sec framework was published on September 2020, followed by a [Cookbook](#) with useful information on how to effectively implement the M-Sec framework on December 2020. Moreover, several scientific articles were drafted by consortium members and presented at international conferences and journals, describing how M-Sec addressed specific needs¹⁷ and the project’s Deliverables were made public in the project’s website and other platforms (Zenodo), containing useful resources and information on the M-Sec framework.

The evaluation of the effectiveness of the activities implemented was assessed within the dissemination and communication KPIs of the project and positive results could be seen through the increasing number of participants attending the Webinars, scientific and non-scientific publications showcasing the project’s initial results, the number of Slack participants and the relevant partnerships made with other EU projects and EU-Japanese initiatives (e.g., EJEa – European Japan Experts Association). Overall, it can be stated that the created and disseminated content supported the marketing goals of M-Sec, with the available content generating new interest from stakeholders on the project’s goals and main achievements.

6.3 Conversion and delight phase

In the conversion phase, that corresponded to the second half of the project’s third year (between March 2021 and September 2021), it was assumed that the project’s main stakeholders were convinced that our solution was the answer to their challenges and the focus was thus on providing clear reasons for them to decide to invest on M-Sec as the smartest thing to do. This phase overlapped with the delight phase, as at the same time clients and stakeholders were asked to provide feedback and generate new content and referrals to other potential users of the M-Sec framework.

Within the timeline of the M-Sec project implementation, the consortium produced documentation on the Use Cases, namely on the problems and challenges, how they were addressed and what could be the next future steps (with a replication focus). Blog posts were drafted, made public and disseminated in the project’s website, social media, and other online channels. These were followed by videos on each Use Case, with testimonials from the consortium and feedback from end-users on the need of M-Sec and the applicability and usefulness in other cities and contexts¹⁸. Additionally, a [comic book](#) was drafted, both in English, Spanish

¹⁵ <https://www.msecproject.eu/m-sec-and-standict-eu-collaboration/>

¹⁶ <https://www.msecproject.eu/m-sec-highlighted-by-cyberwatching-eu/>

¹⁷ The full list can be found at <https://www.msecproject.eu/press-coverage/>

¹⁸ The Use Case videos can be found on M-Sec’s [YouTube channel](#)





and Japanese to reach a larger audience, explaining the clear reasons why M-Sec should be considered the best solution to solve security and privacy issues, by resorting to everyday life examples.

As the [M-Sec Marketplace](#) was launched, the project conducted a marketing campaign that involved a public Webinar, website updates (including a blog post) and social media posts to raise awareness to potential clients of the Marketplace. Moreover, an [Online Contest](#) was held between the 6th and 10th September, with the goal of engaging the industrial and academic sectors towards the adoption and/or development of M-Sec project findings that supported the creation of new business ideas (thus going beyond the project's Use Cases) that addressed the smart cities challenges of Santander and Fujisawa. As part of the Online Contest, contestants were required to demonstrate the novelty of their business idea and its relevance for solving a smart city challenge. Furthermore, contestants needed to also describe how their business idea would be implemented and scaled as a real business solution and how the integration of the M-Sec framework would impact the security and privacy component of that business case.

Finally, a [consultation survey](#) was launched to all citizens and stakeholders with the main goal of collecting feedback on the experience of potential users of the M-Sec solution when using IoT devices and applications and on their knowledge of EU and Japan's data protection regulations. The objective was to help the project better understand the IoT ecosystem in which M-Sec was expected to operate. 350+ answers were provided.

6.4 Relation with business model canvas

This plan was aligned with M-Sec's business model canvas as most of the marketing activities mentioned are considered there. The four phases – awareness, evaluation, conversion, and delight – are primarily executed in the context of the “channels” and “customer relationships” sections. However, the marketing strategy is transversal to the whole business model canvas, it was designed based on the canvas decisions, and the feedback from the marketing activities (e.g., consultation survey, Webinars, Use Case surveys to end-users, etc.) provided data to revisit the business model canvas.

6.5 Potential activities to be conducted after project ending

As the M-Sec project ends on the 30th of September 2021, a set of activities is foreseen to wrap-up and close the project in terms of dissemination and communication of its results:

- The project would like to release a wrap-up video with the main highlights and achievements of the project to feature on the website, YouTube, and social media channels.
- A blogpost is also being considered, with the main takeaways provided by the Project Coordinator, with dissemination at M-Sec's social media channels.
- A final Newsletter is expected to be released, with the wrap-up video, blogpost, and final message from consortium partners.
- The M-Sec website will be revised to its final version and stay online for three years, so that potential users or stakeholders can learn more from the project findings and get in touch with the M-Sec consortium for more information on the Marketplace or future potential partnerships. The final version of the website will include contact details, resources highlight, overview of the overall achievements of the project and future next steps.
- All public Deliverables, as well as scientific publications and other relevant material (i.e., comic book, white paper, cookbook, etc.) will be included in M-Sec's Zenodo account and matched with OpenAire platform, to enable open access and reuse of the research data generated by the project.





- Partners are also encouraged to continue to participate in external events and meetings to present and share project findings, such as the collaboration with Takamatsu Smart City Initiative, in Japan, to organize a joint workshop in the scope of EJEA's Annual Conference, in October 2021, that is expected to join together several smart cities, including Santander and Fujisawa, to share their projects and initiatives and discuss the future of smart initiatives and the role of privacy and security in highly-connected cities and citizens.





7. Conclusions

This deliverable is the last one resulting from the work done within T5.2 Exploitation and IPR activities. However, the completion of the EU-funded project is not the end of the story for M-Sec. On the contrary, the project enters a new stage with plenty of new opportunities.

During this third year, the consortium has been focalized in identifying:

- the M-Sec core components vs extensions components based on the requirements & security threats coverage,
- the market context of the project, such as competitors and trends (Updates on the Market Size & Competitive Landscape),
- the definition of the value proposition provided by M-Sec per each of the stakeholders identified (M-Sec Value Proposition & Relevant Stakeholders) as well as
- the Business Model Canvas and finally on defining and applying the strategy to guarantee exploitation and sustainability of the M-Sec project (M-Sec Exploitation and Sustainability Strategy) where each partner put in place the individual exploitation and commercialization strategies as well as the plans to keep components sustainable for at least 12 months after the project ending.

Use Cases implementation are also one of the drivers to guarantee exploitation activities, for that a Value Proposition and a Business Model Canvas is provided in order to boost replicability. Furthermore, each one of the pilots has clearly demonstrated the value that M-Sec technology can bring in terms of security in the context of smart city. Some use cases owners, as it is the case for UC2, are already exploring how to go further with this technology, both with extended functionalities beyond the current MVP and with different partnerships to complement or complete the current pilot.

In addition, by keeping the different M-Sec components live for at least the next 12 months after the project conclusion, the consortium seeks to find new opportunities either in ongoing or future R&D projects or in terms of commercialization activities from stakeholders that could be interested to explore the M-Sec technology.

Most of the partners are already exploring ways to re-use or continue evolving M-Sec outcomes, such as for academia knowledge transfer and training, further R&D collaboration projects for M-Sec applicability like in the case of TruBlo Project.

Last but not least, the team spirit and the excellent relationship created among the M-Sec partners during these three years is a guarantee for the continuity of M-Sec in many different ways and formats.

