Multi-layered Security Technologies

for hyper-connected smart cities

D56: Market Analysis and Exploitation – 1st year

June 2019

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	D5.6 Market Analysis and Exploitation – first year
Work Package	WP5
Submission date	June 2019
Deliverable lead	WLI /NTTDMC
Authors	All partners
Internal reviewer	ICCS/NTTE
Dissemination Level	Public
Type of deliverable	R
Version history	- V01, 01/March/2019, WLI, Full ToC - V02, 11/March/2019, NTTDMC, review full ToC - V03, 11/March/2019, ICCS, review full ToC - V04, 11/March/2019,WLI, adopted changes ToC - V05, 19/March/2019, WLI, section 3 (owners from use cases included) - V06, 26/April/2019, NTTDMC, input to section 2.3 - V07, 03/May/2019, TST, inputs to sections 2, 3, 4 and 5.4 - V08, 16/May/2019, F6S, inputs to section 2.1 and 5.6 - V09, 16/May/2019, ICCS, inputs to section 5.2 - V10, 17/May/2019, AYTOSAN, inputs to section 5.3 - V11, 19/May/2019, WLI, contribution to section 1, 2.1, 2.2 and 5.1 - V12, 21/May/2019, CEA , contribution to section 5.5 - V13, 22/May/2019, WLI, inputs to section 2.1 and 2.3 - V14, 22/May/2019, Japanese partners, contributions to section 2.2 and 5 - V15, 27/May/2019, WLI, section 2.4 and 4.4 - V16, 28/May/2019, TST, section 5.4 - V17, 3/June/2019, F6S, section 5.6 - V18, 6/June/2019, Japanese partners, section 2, 3 and 5 - V19, 6/June/2019, WLI, review structure and add some comments. - V20, 17/June/2019, AYTOSAN, section 5.3 - V21, 19/June/2019, ICCS, internal review - V22, 20/June/2019, NTTE, internal review - V23, 20/June/2019, NTTDMC, section 2.2

-V24, 25/June/2019, WLI, version ready for submission
-V25, 27/June/2019, WLI, review format
-V26, 28/June/2019, WLI, Final

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).

Table of Contents

List of Tables

List of Figures

Glossary

AI	Artificial Intelligence
API	Application programming interface
Bn	Billion
CPS	Cyber Physical system
CRM	Customer Relationship Management
CS	Customer Segment
CSI	Cyber Science Infrastructure
CTG	CELESTIA Technologies Group
D	Deliverable
DAG	Directed Acyclic Graph
DDoS	Distributed Denial of Service
DKMS	Distributed, knowledge and Media System
EU	Europe
ETSI	European Telecommunications Standards Institute
HW	Hardware
ICN	Information Centric Network
ICT	Information and Communication Technologies
IoT	Internet of Things
IPR	Intellectual Property Right
M2M	Machine to Machine
M	Month
Ms.C	Master of Science
NIST	National Institute of Standards and Technology
OEM	Original Equipment Manufacturer
PaaS	Platform as a service
P2P	Peer-to-peer
Ph.D	Doctor of Philosophy
PIPA	Personal Information Protection Act
QoF	Quality of Life

R&D	Research and Development
SaaS	Software as a Service
SDG	Sustainable Development Goal
SDK	Software Development Kit
SME	Small Medium Enterprise
SoS	Systems of systems
SW	Software
SWOT	Strengths, Weaknesses, Opportunities, Threats
T	Task
Telcos	Telecommunication Company
W3C	World Wide Web Consortium
WP	Work Package

1. Introduction and scope

1.1 Introduction

The goal of this deliverable is to provide an initial view of the market possibilities for a solution like M-Sec, both at a project level and at each individual partner.

This deliverable is structured as follows:

Section 2 "Market research", starts by exploring the current state of art of IoT platforms focused on smart city. Afterwards, similar initiatives and projects within the same framework than M-Sec are shown in order to have a better approach of what already exists or it is currently being developed and what M-Sec could offer as a differentiator factor. It then moves to the analysis of the M-Sec SWOT. The SWOT analysis is a valuable tool to understand and develop a sustainable niche of M-Sec within the market by identifying the strengths, weaknesses, opportunities and threats. Finally, a value proposition for M-Sec is included within section 2.

Section 3 "Business Model for use cases" explores how the six use cases could evolve towards future real businesses. The Consortium has opted for the business model canvas tool to visualize what is important and which key areas to address.

Section 4 "Exploitation of the common platform" gives an initial approach about sustainability of the M-Sec platform after the project has concluded and IPR status both from the assets generated before the project and those ones developed within the project.

Section 5 "Individual exploitation plan" explores the potential innovation but from the view of each of the consortium partners, both within the project timeline and after its conclusion.

Finally, the document includes a point on conclusions and next steps (see section 6) that highlights our understanding of the achievements currently achieved and the tasks where we should focus for the next phases of the project.

This deliverable is a live document following an iterative approach and thus it is going to have a final version on M36 which will include the updated exploitation activities.

1.2 Relation to other WPs and Tasks

“Task 5.2 Exploitation activities” receives input from WP2 and in particular from Tasks “T2.1 M-Sec use case description” and “Task 2.2 M-Sec Pilots: definition, setup and citizens involvement” through the corresponding deliverables (D2.1 and D2.2), input that has been used to develop the corresponding business model canvas for each of the use cases to be implemented in the two smart cities.

At the same time, “Task 5.1 Dissemination and communication activities” and “Task 5.4 Community building and sustainability activities” is in close alignment in the sense that both constitute the foundations of creating awareness of project results and succeed on the exploitation activities.

Furthermore, Task “3.2 M-Sec Architecture” and the whole “WP4 Multi Layered Security” contributes on the identification of assets generated before and through the project as well as IPR issues related.

2. Market Research

2.1 Market benchmark of IoT platforms for smart cities

Today, smart city platforms provide a foundation for urban infrastructure, applications, and services, plus several city-specific functions to address a wide range of city challenges: public safety, waste and water management, traffic and parking, transportation, air quality monitoring, administrative services, public works, tele-assistance and social services, adaptable allocation of city resources, municipal Wi-Fi, and more.

The current market covers basic IoT platforms providing a starting point for cities but mostly these solutions are generalist and do not address city specific requirements like the integration with open data lakes or citizen engagement applications.

The needs of the city will drive the selection and adoption of smart city platforms. Some cities will focus on specific problems as traffic management and will opt for application-specific platforms. Others will choose a generic multifunction platform with a wide range of IoT-enabled services to address all kind of city issues. In any case, there will be always the need to add new solutions and services to the chosen platform and therefore comply with industry standards that may assure a rapid adoption and integration. The smart cities vertical is increasingly dominated by open source platforms allowing the deployment of vendor-agnostic, holistic, and cross-vertical solutions and services and initiatives from FIWARE, ETSI, and W3C are starting to gain traction.

Integration and convergence between IoT and other technologies is also one of the main drivers today: blockchain, AI, multi-cloud environments, edge and fog computing, digital twins, sensor data crowdsourcing or augmented reality to name a few are shaping the market and leading to new business models and partner ecosystems. This is precisely the domain of the M-Sec project and thus, we will focus the benchmark on this path.

This benchmark can tell us that there is no single IoT platform that serves all needs in the smart city scope. Even though a holistic view is required, every city is different and so there are their requirements, priorities and focus. Nevertheless, the convergence of IoT, blockchain, AI and sensor data crowdsourcing is creating a new urban economy by sharing and making all this data available to citizen and service providers to enable new business models.

The use cases defined at M-Sec have their similarities with others already treated independently with some IoT platforms today: air quality and pollution monitoring, health remote monitoring and tele-assistance, waste management, smart buildings, etc.

A recent study report from ABI Research [1] classifies the smart city IoT platform providers in several categories:

Table 2-1: Similar Project References

IoT Platform Category	Vendors	Description
Cross-vertical IoT Platform	Cisco, Verizon	Functionality across verticals (traffic, waste, etc.)
Cross-technology IoT Platforms	IBM, Bosch	Integration with AI, blockchain and sensor data crowdsourcing
IoT platforms from Carriers	Ericsson, Hitachi, Huawei, ZTE	Network infrastructure suppliers and others which are generic and horizontal, do contain some functionalities in targeting the smart city market but essentially don't have what the market seeks
Vertical Smart City IoT platform	Itron, Siemens, Schneider Electric, GE, and Hitachi	Smart buildings, energy efficiency, utilities, public transportation and more. However, ABI Research points out, these are rather more focused on OT (although we would say several are very focused on not just OT and the integration of IT and OT but increasingly on IoT as silos come down in specific of these verticals and even across several of them).
Smart City Applications	Amazon, Azure, SAP, NEC, Microsoft, HPE, NVIDIA, Telit, Carriers, Philips	Broad variety of smart city platforms around products and technologies: solutions built around cloud technology, IT, AI surveillance, connectivity modules), mobile connectivity, and smart lighting.
Open Source, vendor-agnostic standardized IoT Platform	InterDigital	InterDigital's Chordant *(with adherence to the one M2M standard and FIWARE's open source API approach)*. The open source API approach of Chordant revolves around the enablement of applications and services as the focus further moves to gradual deployments, starting from the individual smart city needs and allowing for a degree of readiness for future developments, solutions and growth with urban needs at the centre.

In the context of a M-Sec platform, Verizon, Bosch, IBM and Interdigital lead in the way they support urban technology deployments and should be considered the main IoT platforms base this benchmark, with special

emphasis on Interdigital's Chordant solution for its ability to unlock value from any data source allowing them to build smart city solutions using a best-in-class, standards-compliant and easily deployable platform.

2.2 Similar initiatives and solutions

FIWOO

FIWOO [2] is based in a set of Open Source solutions totally integrated in the platform. FIWOO is a Smart City Platform built under open source ecosystem. It facilitates the integration with IoT-based intelligent applications using FIWARE Open Source technologies like the FIWARE IoT Agent, Orion Context Broker and Perseo CEP. Other Open-Source solutions included in the FIWOO Platform are Docker, CKAN, OpenStreetMap, Jitsi or Kubernetes.

Rambus CryptoManager IoT Security Service for Smart Cities

The Rambus CryptoManager IoT Security Service [3] is a turnkey solution for smart city service providers and OEMs. The solution includes seamless device-to-cloud secure connectivity, device lifecycle management, and advanced device monitoring capabilities to protect service high-availability and help mitigate a variety of attacks including distributed denial of service (DDoS).

The CryptoManager IoT Security Service is comprised of a client software development kit (SDK) that is pre-integrated with the chipset SDK and IoT PaaS provider to enable an easy to deploy security solution. When a supported device is first powered up and connected to the internet, it is automatically identified and authenticated by the solution. IoT Security Service utilizes the IoT device root of trust to authenticate the device, provisions it with certificates to enable the secure connection between devices and the IoT service, and facilitates service providers to manage the security lifecycle management of their devices.

Fybr

Fybr [4] has taken meticulous care to be one of the most secure Smart City service providers in the industry. The company's technology stack has a proven track record of safety and elite protection. Fybr's end-to-end encryption uses NIST-approved algorithms to keep data flowing securely through our network. In addition, the sensors use unique device keys and time-limited session keys. In the unlikely event of a sensor being compromised, it will not affect any other sensor or Fybr gateways. Fybr took a holistic approach to security design from the beginning.

IOTA to Power the Machine-to-Machine Economy

IOTA [5] combines Internet of Things (IoT) with Distributed Ledger Technology to power the machine to machine (M2M) economy. In other words, they'll put microchips in everything, allowing machines to communicate with each other. Think "ownerless taxis" that drive people around, pay the solar charging staging directly, and get repairs all on their own.

Instead of a blockchain, the IOTA network is powered by a Directed Acyclic Graph (DAG) called the Tangle. Essentially, transactions are verified by referencing 2 prior random transactions. DAGs, like the one

implemented by IOTA, boast extremely high throughput, which would be required to connect all devices on the planet.

IOTA partnered with Taiwan to become among the first blockchain-based smart cities [6]. In Taiwan, IOTA is creating an ID-management system called TangleID. This project was designed to decrease identity theft, minimize voter fraud, distribute medical records, access social security, etc.

IOTA recently announced a pilot project helping 5 cities in the EU becomes “energy positive” [7]. In other words, these cities are attempting to produce more energy than they consume.

Waltonchain Provides a Secure Value Transport Layer

Waltonchain [8] is a heavyweight in the Smart City Revolution, and is projected by many to be a top 10 project by 2020.

Waltonchain is both a hardware (microchips) and software (blockchain) project offering a wide range of solutions perfect for powering a smart city.

The Waltonchain network is engineered for parallel side-chains, which allows for many enterprises to interact on the same network while maintaining the high throughput required supporting IoT initiatives.

In terms of smart cities, Waltonchain has announced several projects in both China and Korea, including: smart sanitation, smart resource optimization, maritime port management, and more.

China is sponsoring the creation of 500 smart cities to support the rapid urbanization they’re forecasting, and Waltonchain is right in the middle of this massive initiative. In fact, Citilink Technology (a Walton subsidiary) created an award-winning Smart Waste Management System being run on top of Waltonchain.

Meanwhile, Waltonchain has partnered with Alibaba Cloud (Aliyun) to implement smart cities in China, with a focus on Xiong’an and Yuhang. Alibaba is contributing cloud computing and artificial intelligence while Waltonchain is adding IoT and blockchain technology to support the Smart City Revolution.

Applications initiatives include smart resource allocation optimization, urban management, and business ecosystem redesign.

Power Ledger Offers Decentralized Energy Marketplaces

Decentralized power production and consumption offers tremendous efficiencies as well as makes future cities more resilient.

Perth-based company Power Ledger [9] is a blockchain-based decentralized energy market provider with several smart city pilot projects live around the world. Here are a few examples.

In November 2017, the Australian government announced they would provide funding for a smart city project in Fremantle, Australia. Power Ledger would trial the use of blockchain-based distributed energy and water systems. Specifically, Power Ledger would be the transactional layer for renewable assets (energy and water), and would provide the tech foundation for community-owned battery farms. This allows citizens and private enterprises to produce their own energy (solar panels, etc.) and sell it on a public marketplace in exchange for POWR tokens which can then be used to purchase water or be traded for fiat.

Chariot

Chariot [10] aims to implement a next generation cognitive IoT platform that can enable the creation of intelligent IoT applications with intelligent shielding/supervision of privacy, cyber-security and safety threats, and to complement existing IoT systems in non-intrusive ways and help guarantee robust security. Chariot uses blockchain to record and affirm/approve IoT physical, operational and functional changes through a cognitive engine and private keys to prevent malicious changes. A Fog decentralised infrastructure guarantees Firmware Security integrity by using blockchain to enhance physical, operational and functional security of IoT systems. An IoT Safety Supervision Engine provides a novel solution to the challenges of securing IoT data, devices and functionality in new and existing industry-specific safety critical systems.

SerIoT

SerIoT [11] aims to provide a useful open & reference framework for real-time monitoring of the traffic exchanged through heterogeneous IoT platforms within the IoT network in order to recognize suspicious patterns, to evaluate them and finally to decide on the detection of a security leak, privacy threat and abnormal event detection, while offering parallel mitigation actions that are seamlessly exploited in the background.

SecureIoT

SecureIoT [12] project focuses on delivering predictive IoT security services, which span multiple IoT platforms and networks of smart objects and are based on security building blocks at both the edge and the core of IoT systems. Foretelling and anticipation of security behaviour of IoT entities, is the main concept emphasised by SecureIoT. The provided services span security compliance auditing, automated risk assessment and mitigation, as well as support for IoT security-aware programming.

IoT Device Security Manager

It is whitelist type access control software that protects the customer system from various threats of IoT occurring on edge and devices. Security risks for IoT systems, such as the ability to automatically create, in the form of whitelists, security settings for each device distributed in large numbers in places that are difficult to use manually, as well as remotely visualizing the connection and communication status of IoT devices in the field can be reduced. [13]

SecureWare/Credential Lifecycle Manager

SecureWare [14] is a software that includes creation and management of device ID, encryption key (public key / common key) and electronic certificate necessary for mutual authentication and encryption to prevent unauthorized connection.

Finally, in the following table you will find other initiatives in smart city context:

Table 2-2: Similar Project References

Project	URL	Platform
Brain-IoT	http://www.brain-iot.eu/	Brain-IoT [15] aims at establishing a framework and methodology that supports smart autonomous and cooperative behaviours of populations of heterogeneous IoT platforms that are also closely interacting with Cyber-Physical systems (CPS).
bIoTope	https://biotope-project.eu/overview	BIoTope [16] lays the foundation for creating open innovation ecosystems by providing a platform that enables companies to easily create new IoT systems and to rapidly harness available information using advanced Systems-of-Systems (SoS) capabilities for Connected Smart Objects.
Decenter	https://www.decenter-project.eu/	DECENTER [17] is a research and innovation project aiming to deliver a robust Fog Computing Platform, covering the whole Cloud-to-Things continuum, that will provide application-aware orchestration and provisioning of resources, driven by methods of Artificial Intelligence. The underlying infrastructure will span across borders into a federation, and will utilize Blockchain and Smart Contracts to reach secure processing, automated operation and timely delivery of responses.

2.3 M-Sec SWOT analysis

A SWOT (strengths, weaknesses, opportunities and threats) analysis has been conducted in order to identify and analyse the internal and external factors that can have an impact on the viability of the M-Sec platform. Overall, the SWOT provides a list of barriers (weaknesses and threats) and drivers (strengths and opportunities). As this deliverable is a first version of the Market and Exploitation Plan and WP4 have just started two month ago, a technical point of view for the SWOT analysis will be considered and taken into account in the following versions of this deliverable.

- Strength
  - Support for further smart city domain protocols and platforms.
  - Scalability and Interoperability.
  - Open source technology.
  - Support for publish/subscribe and client—server type of protocols.
  - Well-defined data and service model.
  - Processing at the edge side.
  - Advanced data processing.
  - Possibility of programming applications that would run on the platform with actuation possibilities.
  - Participation of multiple partners with different expertise facilities the building of a robust platform and open opportunities for future collaborations especially on the sustainability of the platform.

- Weakness
  - Support, maintenance and operational costs.
  - Securities of the involved systems which are developing are not guaranteed.
  - Sustainable concrete and clear business model.
  - Unclear roadmap for technology adoptions.

- Opportunity
  - Rapid growth of IoT devices. Estimated to increase from 7B (2018) to 22B by 2025. [18]
  - Changes in data privacy law.
  - Low competition offering the same type of concept. Most of the platforms don't include an end to end multi security layer.
  - Increase of ATTACKS AGAINST Internet of Things (IoT). Last year, 32.7 million IoT attacks were detected [19]. Due to the high number of IoT attacks, solutions like M-Sec can be really well received in the market.
  - Technical expertise from partners in different security layers.
  - Data collection and distribution with a unified way of accessing to underlying heterogeneous data sources.
  - Rapid and simple development of end-user applications.
  - Needs to utilize the IoT and Blockchain systems to make operation efficient.
  - Test and validation to ensure things adaptable to citizens.

- Threats
  - No funding beyond the length of the project.
  - Platform sustainability once the project has finalized.
  - Functionalities issues by integrating all the security layers.
  - Increase of ATTACKS AGAINST Internet of Things (IoT). Last year, 32.7 million IoT attacks were detected [19]. Despite the security measures implemented by different solutions in the market, the volume of attacks is still very high.
  - There are currently more than 360 IoT platforms in the market, of that number more than 60 are targeted specifically at the smart city [20].
  - Cities worldwide could waste as much as $341bn by 2025 if they adopt a fragmented approach towards IoT as opposed to as standardized one [20].
  - Large wave of urbanization. Cities need to unlock the value of data.
  - Impact of data is strongly connected to an effective data collection, management, processing and interpretation.
  - Evolving security threats.
  - Highly Innovative concept.

2.4 M-Sec positioning and expected value proposition

Most of the platforms identified in section 2.1 Market Research tend to be built around the concept of IoT/cloud convergence, which foresees the integration of heterogeneous data streams within one or more cloud infrastructures promoting a centralized data collection and processing approach, which introduces several limitations both in terms of the supported applications and in terms of the business models that they enable.

In particular, smart city platforms are mainly centralized IoT/Cloud infrastructures and thus they tend to be:

- Inefficient in handling actuation such as use cases involving invocation and control over sensors and physical devices.
- Prone to “complete failures” since they dispose with centralized control by a limited number of administrative entities (e.g., service providers, smart cities, service operators).
- Inherently insecure by their centralized approach, more sensible to systems hacking attacks, data theft and data tampering than decentralized platforms
- Inflexible in the incorporation of innovative applications and new business models, mainly because they require heavy administration and do not facilitate peer-to-peer decentralized interactions between people and “things”.
- There is no “platform of platforms” approach, with open, interoperable platforms interacting with and complementing each other in an open ecosystem. Ultimately, this undermines the opportunity for interoperability between two smart city platforms and the exchange of open data in a marketplace context. This inter-city, inter-platform marketplace shall be one of the key points for M-Sec differentiation and value proposition.

As a core differentiator, M-Sec value proposition should be positioned on the aim to provide secure, interoperable interactions between IoT elements based on a holistic secured cloud/edge/IoT context within a future smart city. In modern smart city applications there is an emerging need of end-to-end security since many data sources may contain sensitive information that raises issue on privacy and data protection. The smart city application is inherently multi-layers including edge, cloud and application levels. The security and privacy issues should be addressed in the all layer to ensure “end-to-end security and privacy”.

For instance many smart city applications are utilizing data streams such as images from cameras or mobile applications, and these streams should be protected from attackers in the all layers by, for example, hijack protection mechanism in the sensors devices, secure IoT gateway connecting the devices and cloud, data encryption and access control in the cloud, and secure applications utilizing the data stream. Last but not least, nowadays, a huge number of IoT devices have been attached in smart city environments. These IoT devices are facing a huge number of intrusions and now one of the major sources of springboard attacks in turn. They should thus be monitored by a sophisticated technology to protect them from malware instances for better serving hyper connected cities. At the same time, decentralized data collection and processing bring in new challenges for security and data privacy in overall. Security is core to M-Sec value proposition as a multi-layered security technology to complement mainstream IoT/cloud technologies, through enabling the introduction and implementation of specific classes of applications and services, which are not efficiently supported by state-of-the-art architectures.

Additionally, blockchain ledgers can provide a common reference for distributed and decentralized systems for collaboration increasing the levels of trust in trustless environments. Blockchain technologies at the same time can provide a tamper-proof framework for data to be exchanges between smart city platforms, while forming the underlying technology for building the internet of value that can make a marketplace of sensors in smart city context a reality. By applying the blockchain concept to a highly decentralized IoT, as it is the case with M-Sec, new capabilities are being offered. A smart object, part of smart city IoT infrastructure, can be registered to a regional blockchain and the object remains a unique entity within the blockchain throughout its life.

M-Sec vision is to become an open source smart city platform enacting a marketplace for third parties develop secure applications and services around secure cloud/edge/IoT elements. The final goal for a city to become smart is having access to information, and to use that information to improve citizen services and city operations. In that sense, M-Sec aims to become interoperable for different applications built on top of it responding to vertical needs and at the same time, become interoperable among other smart cities by decentralizing the access to data and information from one to the other, and thus, generating new business models based on data sharing.

3. Business models for use cases

In this section, a business model canvas is provided for each of the use cases. In the following points, it is explained the business canvas methodology, a general description of each of the categories displayed in the canvas according to Christopher Bartlett [21].

Value Proposition

It is the fundamental concept of the exchange of value between your business and your customer/clients.

Generally, value is exchanged from a customer for money when a problem is solved or a pain is relieved for them by your business.

Good questions to ask when defining your business/product:

- What is the problem I am solving?
- Why would someone want to have this problem solved?
- What is the underlying motivator for this problem?

Customer Segments

Customer Segmenting is the practice of dividing a customer base into groups of individuals that are similar in specific ways, such as age, gender, interests and spending habits.

Things to consider when determining your Customer Segments:

- Who are we solving the problem for?
- Who are the people that will value my value proposition?
- Are they another business?
- If so, what are the characteristics of those businesses?
- Or, are they other people?
- Does my value proposition appeal to men/women or both?
- Does it appeal to young adults aged 20 to 30 or teenagers?
- What are the characteristics of the people who are looking for my value proposition?
- Another thing to gauge and understand is your market size, and how many people there are in the Customer Segment. This will help you understand your market from a micro and macro perspective.

Customer Relationships

Customer Relationships is defined as how a business interacts with its customers.

Good questions in this category may include the following:

- Do you meet with your customers in person?
- Or over the phone?

- Or is your business predominantly run online so the relationship will be online too?

Channels

Channels are defined as the avenues through which your customer comes into contact with your business and becomes part of your sales cycle.

This is generally covered under the marketing plan for your business.

Good questions to ask when identifying the channels to reach your customers are:

- How are we going to tell our customer segment about our value proposition?
- Where are our customers?
- Are they on social media?
- Are they driving their car and listening to the radio?
- Are they at an event or conference?
- Do they watch TV at 7pm on a Friday night?

Key Activities

The Key Activities of your business/product are the actions that your business undertakes to achieve the value proposition for your customers.

Questions to ask:

- What activities does the business undertake in achieving the value proposition for the customer?
- What is the resource used?
- Time?
- Expertise?
- Distribution of product?
- Technical development?
- Strategy?
- Offer resources (human/physical)?
- What actions does it take you and/or your staff to achieve value exchange?

Key Resources

Key resources are what are needed practically to undertake the action/activities of your business. Key resources could include office space, computers and staff.

Key Partners

Key Partners are a list of other external companies/suppliers/parties you may need to achieve your key activities and deliver value to the customer. These moves into the realm of 'if my business cannot achieve

the value proposition alone, who else do I need to rely on to do it?'. An example of this is 'if I sell groceries to customers, I may need a local baker to supply fresh bread to my store'.

Cost Structures

Your business cost structure is defined as the monetary cost of operating as a business.

Some questions to pose may include the following:

- How much does it cost to achieve my businesses key activities?
- What are the cost of my key resources and key partnerships?
- How much does it cost to achieve the value proposition for my customers/users?
- Are there additional costs to running a business?
- Legal?
- Insurance?
- What is the cost of my business?
- It is important also to place a monetary value on your time as a cost.
- How much would it cost you to hire you?
- What is the opportunity cost of running your business?

Revenue Streams

Revenue Streams are defined as the way by which your business converts your Value Proposition or solution to the customer's problem into financial gain.

It is also important to understand pricing your business accordingly to pain of purchase in exchange for the pain of solving the problem for your customer.

There are many different revenue models here:

- Pay per product (pay per view)
- Fee for service
- Fixed rate
- Subscription
- Dividends
- Referral feeds
- Freemium

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

Business Model Canvas	Designed for:	**Use Case 1 - Reliable IoT devices**
	Designed by:	**TST**

KEY PARTNERS	KEY ACTIVITIES	VALUE PROPOSITIONS	CUSTOMER RELATIONSHIPS	CUSTOMER SEGMENTS
- Municipalities (City Council + Concessionaire companies) and municipal services (CS1, CS2) - Users, as they provide and manage data (CS3, CS4, CS5) -European Union for funding and dissemination - Hardware partners to provide sensors and devices for Pilots 1.1 and 1.2 - European Union for funding and dissemination - M-Sec Consortium partners	- Management of information collected by sensors through the platform. - Study of users acceptance to services innovations - Build the demonstrator and evolve it to a platform (Agile approach) - Get feedback from stakeholders - Evaluate pilots and prepare key messages to "sell it" - Raise investment for product commercialization **KEY RESOURCES** - Sensors and IoT devices - Technical team to develop the demonstrator and evolve it to a pilot and a product	- Someone that needs to perform a lot of experiments could use one specific and well-known tool VP1 (CS1-9): A B2B2C, SaaS-based, IoT platform featuring integrated components to enable solutions useful for citizens and municipal services VP2 (CS1-9): 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 (CS1-9): ensure system resiliency (no single point of failure) and end user privacy VP4 (CS1): Collect real-time, IoT-based data on environmental aspects in the park and crowd counting in different parts of the park	- Helpdesk and support tools to be provided to users - Self service on front end (web, mobile) for all users - Consortium management (i.e. committees) **CHANNELS** 1. Awareness: - Promotional material (Corporate websites, brochures, advertising,...) - News in the local media - Direct meetings with CS1-CS5 representatives - Public conferences, hackathons, workshops and other activities to promote the solution and show examples of success stories 2. Evaluation: surveys and feedback programs via web and face to face. 3. TST Sales 4. After sales: Customer service	**Pilot 1.1 and 1.2** - Municipal services -- CS1: Environmental service - establishing fixed routes and enriching them with useful information -- CS2: Tourist service - getting valid information from the people counter that will help to know the most well received sports in the park by both citizens and visitors - Citizens -- CS3: Elderly - use fixed routes suggested by the app to go for a walk and provide a positive impact in their well being -- CS4: Schoolers - Fixed routes offered by the municipality and put into the application can be used by schools to show their schoolers the different parts of the park and their specifics trees, birds, etc. -- CS5: General public - users can both follow the routes specified in the app and check the number of people in certain spots (helpful to, e.g., avoid them if they are too crowded)

COST STRUCTURE	REVENUE STREAMS
- Deployment maintenance - Employees salaries:11:13product ownership / project management, communication roles, business roles (funding, business model definition and evolution), consortium governance roles and business model expertise - Technical partner cost for maintainng and evolving the platform (Product roadmap) - Dissemination costs (travel, tradeshows, articles, etc.) - Hosting infrastructure - Hardware (device and sensors) acquisition - Customer service	BUILD (Set-up phase): - Initial basic application for free RUN (operational phase): - Entrance & subscription fee - Advanced functionalities fee

Figure 3—1: Use Case 1 Business Model Canvas

3.2 Use Case 2: Home monitoring & well-being tele-assistance for ageing people

Business Model Canvas	Designed for:	Use Case 2: Home Monitoring & Wellbeing Tele-assistance gor ageing people
	Designed by:	Worldline

KEY PARTNERS	KEY ACTIVITIES	VALUE PROPOSITIONS	CUSTOMER RELATIONSHIPS	CUSTOMER SEGMENTS
- 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 for Pilots 2.1 and 2.2 - European Union for funding and dissemination - MSEC Consortium partners	- Build the demonstrator and evolve it to a platform (Agile approach) - Get feedback from stakeholders - Generate awareness about Connected Care, MSEC 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	VP1 (CS1-6): A B2B2C, SaaS-based, IoT platform featuring integrated components to enable tele-monitoring user-centric solutions 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. VP3 (CS1, CS3): provide access to patient/citizen monitoring data to trigger accurate and adequate home care services VP4 (CS1-6): build a network of caregivers to provide monitoring information to the closest relatives VP5 (CS1-6): ensure system resiliency (no single point of failure) and end user privacy VP6 (CS1-6): facilitate direct communication between members of the caregiving network to access first-hand information and fight elderly isolation VP7 (CS1): Collect real-time, IoT-based data on ageing citizens at their homes to provide accurate and rapid tele-assistance supporting services VP8 (CS4): Leverage on IoT devices to collect well-being data (e.g. physical activity, sleep quality…) to monitor and pursue a better healthy behavior. Change people's attitude towards their own health and raise their expectations on living a longer, healthier life	- Global Product Manager as SPOC - Self service on front end (web, mobile) for all 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	**Tele-assistance & Home monitoring (Pilot 2.1)** CS1: Tele-assistance companies - they monitor users at home through IoT sensors CS2: Telcos - they sell their SIMs and communication services to tele-assistance companies. Eventually, they also build a tele-assistance value propositon 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. **Well-being (Pilot 2.2)** CS4: Corporate - they offer wellness and wellbeing services to their employees in so-called wellbeing@work initiatives CS5: Insurance - new business models based on personalization (e.g. pay-as-you-drive) will ultimately arrive to health and wellbeing. This solution will enable new services and benefits based on client's healthy habits CS6: Public Health Services: public administration are offering new services around changing people's attitude towards their own health and raise their expectations on living a longer, healthier life
	KEY RESOURCES		**CHANNELS**	
	- Technical team to develop the demonstrator and evolve it to a pilot and a product - Product ownership / project management roles - Communication roles (stakeholders, press, etc.) - Hosting infrastructure - Funding research to cover the evolution from pilot to product - Consortium governance and business model expertise		1. Awareness: - Pilots with Ayuntamiento Santander & 1 CS1 and feedback from stakeholders. Once we have results we move to the next phases. - direct meetings with existing partners to extend the pilot and with new potenail partners (mostly CS1 &CS3) to invite them to participate in the platform. . - articles 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 web and face to face. 3. Partners (via their sales force) 4. Delivery: via SaaS mode by Worldline 5. Worldline Sales - Global Account & Product Managers 6. After sales: Customer service	

COST STRUCTURE	REVENUE STREAMS
- Technical partner cost for maintainng 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	1. SaaS based business model leveraging on two phases: **BUILD** (Set-up phase): - 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) **RUN** (operational phase): - 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 2. API REST - price based on service consumption

Figure 3—2: Use Case 2 Business Model Canvas

3.3 Use Case 3: Security & trustworthy environment monitoring with automotive, participatory and virtual sensing techniques

Business Model Canvas	Designed for:	**Use Case 3 - Security & trustworthy environment monitoring with automotive, participatory and virtual sensing techniques**
	Designed by:	**KEIO**

KEY PARTNERS	KEY ACTIVITIES	VALUE PROPOSITIONS	CUSTOMER RELATIONSHIPS	CUSTOMER SEGMENTS
- 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 gabage trucks, roard monitoring image Data by camera installed on gabage trucks, river monitoring image from open Data - MSEC Consortium partners	- 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	VP1(CS1-2):Realtime IoT sensing data, for example, air quality VP2(CS1-2):Automatical detection of road damage by deep learning analytics VP3(CS2):Realtime river monitoring data from open web site VP4(CS2):We can provide the realtime data of local air quality which could not provide general web information such as very spot area concerned by customer VP5(CS1-2):We can provide automatical detection of road damage data which enables reduce city officer's effort. VP6(CS2):We can provide river monitoring data as a actual Iot sensing using sensorizer techniques.	- Self Service as a data sharing by using web browser and smartphone apps. - Web browsing and smartphone apps as a frontend of M-Sec platform	CS1:Fujisawa Recycle Coop CS2:Fujisawa City
	KEY RESOURCES		**CHANNELS**	
	- 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 useful information in real time		- 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
- Maintenance cost of M-Sec platform, smartphone apps, server and so on. - System integration and mentainace cost of M-Sec platform	- There is not clear revenue stream yet as a sustainable business model. The estimated ways to make revenue streams by providing users with developing service - Reduction of city officers resourse 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 resourse cost

Figure 3—3: Use Case 3 Business Model Canvas

3.4 Use Case 4: Secure and trustworthy hyper-connected citizen care

Business Model Canvas	Designed for:	**Use Case 4 - Secure and trustworthy hyper-connected citizen care**
	Designed by:	**KEIO**

KEY PARTNERS	KEY ACTIVITIES	VALUE PROPOSITIONS	CUSTOMER RELATIONSHIPS	CUSTOMER SEGMENTS
- Generally, the key partner could be the entity who can provide the data depend on each purpose. For example, it could be Fujisawa Recycle Corp for the purpose of the optimization of urban waste generarion per household. - Fujisawa City and key partners depend on the purposes - Depend on the purposes. For example, counting data of the amount of waste is key resourse for the optimization of urban waste generation per household. - As a data supplyer via M-Sec architecture including "Hyper connected citizen care applications" - MSEC Consortium partners	- Supplying data via M-Sec architecture including "Hyper connected citizen care applications" - 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 "Hyper connected citizen care applications" - Sharing the raw data and the results of analytic data as secure and trustworthy Hyper-connected Citizen Care	VP1(CS1-3):Hyper-connected citizen care by exchanging useful information depend on each purpose via M-Sec architecture including "Hyper connected citizen care applications" as secure and trustworthy connection. VP2(CS2-3):Customer's concern about exchanging various data including their privacy data VP3(CS1-3):M-Sec architecture including "Hyper connected citizen care applications" as secure and trustworthy connection. VP4(CS2-3):Providing secure and trustworthy data exchange platform	- Hyper-connected citizen care by exchanging useful information depend on each purpose via M-Sec architecture including "Hyper connected citizen care applications" as secure and trustworthy connection. - M-Sec architecture including "Hyper connected citizen care applications" as secure and trustworthy connection.	CS1:Fujisawa Citizens CS2:Fujisawa City CS3:Key partners who depends on each purpose
	KEY RESOURCES		**CHANNELS**	
	- M-Sec platform as a secure data distribution and exchanging platform "Hyper connected citizen care applications" as a frontend of M-Sec platform - Customer can refer useful information in real time as secure and trustworthy Hyper-connected Citizen Care		- Ideally, establishment of the channels structure including revenue mechanism enables sustainable business model is important. - There is just data sharing by M-Sec architecture including "Hyper connected citizen care applications". - There is not integrated channels yet.	

COST STRUCTURE	REVENUE STREAMS
- Maintenance cost of M-Sec platform, "Hyper connected citizen care applications", server and so on. - System integration and mainteinace cost of M-Sec platform	- There is not clear revenue stream yet as a sustainable business model. The estimated ways to make revenue streams by providing users with developing service - Reduction of city officers resourse 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 resourse cost

Figure 3—4: Use Case 4 Business Model Canvas

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

Business Model Canvas	Designed for:	Use Case 5 - A marketplace of IoT services for effective decision making
	Designed by:	NTTE

KEY PARTNERS	KEY ACTIVITIES	VALUE PROPOSITIONS	CUSTOMER RELATIONSHIPS	CUSTOMER SEGMENTS
- M-Sec partners - Security techniques - To provide security techniques - Enterprises as buyers or sellers - School - Parents - Public	- Management of the platform, database, users data, update on security techniques - To get agreement from users or the parents before using the app - To translate original languages into their own ones. - develop the application for web browser or both iOS and Android to use Smile wave application - No pictures of face will be stored	VP1(CS2-4):marketplace where they can get trustworthy data in a secure way when they want it VP2(CS1-4):Gurantee 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(CS1,4):Can get trustworthy data efficiently VP4(CS2-6):Can be translated into their own languages VP5(CS2-3):Can provide data only to whom they want to provide, Want to get money by selling data Offering: VP6(CS1-6):Secure and trustworthy data marketplace	- To be trusted by managing and maintaining stable marketplace, Guarantee security - To be trusted by securing the individual information considering GDPR and PIPA	Buyer CS1:Enterprises who want to buy data (consulting firm, data analysis, marketing research, ad agancy, municipality) Seller CS2:Enterprises or person who want to sell data (consumer, general company which has data, consulting firm) CS3:consulting firm, marketing research company Others CS4:Public CS5:private school CS6:Parents or Users oneself
	KEY RESOURCES - Security know-how, blockchain, human resources (system design, management, support), multi-layered security technology, cloud server, payment system - KEIO smile wave application - ICCS block chain system		**CHANNELS** - Trustworthy way, Recommendation from government, school, Authentication from credible organization, Exibit in events organaized by government or credible organization related to security	

COST STRUCTURE	REVENUE STREAMS
- labor cost - service management & maintenance cost - lisence fee - promotion cost - R&D cost	Customer's viewpoint: - Buyer: Data sold by companies, Get data by taking their labor, Monetary reward for answerers to questionnaires - Seller: Fee to participate in marketing research network User's viewpoint: Buyer: Cheaper/more cost-saving than current process Seller: Can easily get money by selling data Revenue compositons ratio: Marketplace membership fee (defferent membership level) (40%), Service charge (40%), Advertisement revenue (20%) Way to pay: - prefer Credit card, QR payment to Cash

Figure 3—5: Use Case 5 Business Model Canvas

3.6 Use Case 6: Citizens-as-sensor

Business Model Canvas	Designed for:	**Use Case 6 - Citizen as sensor**
	Designed by:	**TST**

KEY PARTNERS	KEY ACTIVITIES	VALUE PROPOSITIONS	CUSTOMER RELATIONSHIPS	CUSTOMER SEGMENTS
- Municipalities (City Council + Concessionaire companies) - Users, as they provide and manage data -European Union for funding and dissemination	- Management of information collected by the app. - Study of users acceptance to services innovations - Study of users acceptance to services innovations - Get feedback from stakeholders - Evaluate pilot and prepare key messages to "sell it" - Evaluate possibilities for cross-border product commercialization	VP1 (CS1-4): A B2B2C, SaaS-based, IoT platform featuring integrated components to enable citizen participation in the city daily operations and make them feel they are contribution to the city progress VP2 (CS1-4): 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 (CS1-4): provide citizens with monitoring data and functionalities to trigger accurate and adequate actions from the municipal services VP4 (CS1-4): ensure system resiliency (no single point of failure) and end user privacy	- Helpdesk and support tools to be provided to users - Self service on front end (web, mobile) for all users - Consortium management (i.e. committees)	- Municipal services -- CS1: Tourist service - getting valid information from theapp that will help to know the most well received spots in the city by both residents and visitors -- CS2: Geneal Municipal services - acting upon certain citizen demands received through the application - Citizens -- CS3: Residents - highlighting their preferred city spots and warning about issues to solve in certain parts of the city -- CS4: Visitors - naming and commenting their favorite city points of interest
	KEY RESOURCES		**CHANNELS**	
	- Mobile app (interacting with some IoT devices) - Technical team to develop the demonstrator and evolve it to a pilot and a product		1. Awareness: - Promotional material (Corporate websites, brochures, advertising,...) - News in the local media - Direct meetings with CS1-CS4 representatives - Public conferences, hackathons, workshops and other activities to promote the solution and show examples of success stories 2. Evaluation: surveys and feedback programs via web and face to face.	

COST STRUCTURE	REVENUE STREAMS
- Deployment maintenance - Employees salaries:product ownership / project management, communication roles, business roles (funding, business model definition and evolution), consortium governance roles and business model expertise - Technical partner cost for maintainng and evolving the platform (Product roadmap) - Dissemination costs (travel, tradeshows, articles, etc.) - Hosting infrastructure - Customer service	BUILD (Set-up phase): - Initial basic application for free RUN (operational phase): - Agreement with Municipalities to deploy the same system in different cities

Figure 3—6: Use Case 6 Business Model Canvas

4. Exploitation of the common platform

4.1 Use Case driven exploitation

The M-Sec project is composed by six use cases that share strong common requirements (as it is described on deliverable D3.1 Requirement Analysis).

We started by identifying the main functional and non-functional requirements per use case as well as for the M-Sec platform.

Once we had this information, the next step is to make an exercise to gather those functionalities in potential shared modules (i.e. common API), accessible by all use cases as they may need them.

Therefore, while we are designing a platform that produces modules accessible by all six use cases, each use case could obtain similar or completely unique functionalities from those modules.

Exploitation of M-Sec results for the industrial partners involved will come from future products evolved from the technology integrated into the use cases and from the overall M-Sec concept, which will introduce a novel security layer into their respective IoT devices portfolio.

4.2 Common assets

Within deliverable D3.3 M-Sec Architecture, assets previously generated by partners are identified and matched accordingly with its related use on the different use cases. No IPR issues have been stated by any of the partners who made the M-Sec consortium.

4.3 Sustainability of the platform

The M-Sec platform so carefully designed, built and tested along the course of the project looks to become a solution with high market potential, which would help consortium members to exploit it. However, all effort of having a robust and a design platform adapted to the requirements of each use case is useless if M-Sec cannot ensure its continuous availability not only during the length of the project but also after its conclusion.

In order to do so, partners in the M-Sec consortium will need to delve into what they consider the best practices to adopt in its sustainability model, and recap, after the different stages of the Use Cases deployment are completed, which tools were preferred and/or better perceived by users interacting with them during the diverse experimentation stage and how they used them.

A business model describes the rationale of how an organization creates, markets, delivers and captures value. Nowadays, business model innovation is often more important than a better idea or technology. A suitable business model depends on different factors, the character of the stakeholders taking part in the network being one of the main ones. When coming to a decision with respect to the specific business model

to adopt, an additional relevant point to take into account by M-Sec consortium consists of the peculiarity that M-Sec offers a complete solution, not just a platform but also several components and APIs that help future users to carry out their projects, which is something new in today's market context, an aspect that has an influence over M-Sec's value proposition.

4.4 Innovation & IPR Management Strategy

At this point of the project (M12), the consortium has identified a number of assets to bring to the project, which also defined the respective owners (partners) and how are related with the different use cases. Currently, none of the owners are reporting any critical IPR issues related to their components. However, during the length of the project and with WP4 Multi Security layers having start in M10, the consortium will conduct further IPR management activities and hold discussions related not only to the components already generated before the project but also with the ones that will be generated. For that, a template will be generated for this purpose, which will cover Innovation Type, Version Status, Planned Licences, use by Partners and Use Cases, Description, IPR opportunities and Application Area.

The results will be included on the next deliverable from T5.2 Exploitation and IPR activities to be submitted by the end of M24 and M36.

5. Individual exploitation plans

5.1 Worldline

Business objectives in the project

Worldline, apart from being the European Coordinator, it also acts as one of the technical partners, contributing to identifying the requirements that must be covered by 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 assistance solution is also the owner of the Home Monitoring & Wellbeing Tele assistance use case (Use case 2).

If we focus on Worldline individual exploitation plan, we can talk of the following business objectives around the participation in the M-Sec project:

- To maximize the technical and business expertise around the development of P2P level security and blockchain as well as application level security.
- To develop technical assets that could be used later in future versions of the project or in other R&D and commercial offers.
- To position itself as the ideal technical and business partner, thus creating the basis for future collaborations in Blockchain or other emerging technologies.
- To expand Worldline Business Portfolio not only in home and wellbeing domain but also in the health sector by evolving Connected Assistance to Connected Care which will include not only more functionalities but also a key differential added value by integrating security and privacy layers.

Innovation and exploitation possibilities

Worldline is the biggest European payment services provider and a leader in digital transformation. With annual revenues of €2,3 Bn and +11.000 employees worldwide, it specializes in the development of cloud-based platforms that customizes for its clients and exploits through transactional business models (i.e. pay per use) [22].

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

Finally, Worldline invests very heavily on Research & Development, both via internal projects and via collaborative ones such as the ones included in research programs such as 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 M-Sec- platform or applying the developed assets to other projects.

Innovation & exploitation during the project (overall plan throughout the whole duration of the project)

The innovation and exploitation possibilities to be explored during the 3 years of the M-Sec project are the following:

- During the first year Worldline has explored the current home monitoring and wellbeing tele assistance solutions that already exist in the market with the aim of providing a solution that ideally covers all the main business aspects and user needs.
- Meetings with potential suppliers of IoT devices have taken place in order to find a provider who offers affordable devices while at the same time provides high standards on usability and quality.
- A product portfolio based on the evolution of the "Connected Assistance Platform" to the "Connected Care Platform" has been done in order to display all the use cases that are applicable for our target customers. In addition, Worldline has developed a business model to exploit Connected Care Platform. The Business Model is based in an operational fee (users/month). Furthermore, the platform could be commercialized as a white label or can be customized by adding branding, integrations, new features, and so on.
- M-Sec project and Connected Care have been presented both within the Atos and Worldline groups as well as to external clients, as a way to express Worldline's capabilities. Worldline has encountered several potential collaboration opportunities around providing security layers on home and health monitoring. For instance, Worldline has conducted several meetings with TiC Salut (public entity that promotes innovation and technology around the health sector). TiC Salut is very interesting on how blockchain can be applied on health. On that way, Worldline could take advantage to conduct a pilot on health taking advantage of the M-Sec platform as a way to secure all data collected.
- Worldline has initially agreed with the rest of the consortium partners 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.
- On the next two years, Worldline will pursue the following objectives:
    - To gain strong expertise in aspects such as Blockchain.
    - The creation of a serie of digital assets that may be used to accelerate the development of solutions for third parties.
    - To continue pushing the M-Sec project and the Connected Care Platform to Tele-assistance companies, Telcos, Public Social Services, Public Health Services, Corporate companies, Insurance and Pharma, University and Research Centers. Both existing customers and potential leads for them to participate in the project and/or to explore similar solutions.
    - To establish a strong feedback and improvement cycle around the M-Sec platform and pilots tested. This will allow the consortium to learn what it works and what needs to be mended.
    - To position Worldline as a leader among its peers, since not many companies would count with the experience of implementing a real life project internationally. At this stage,

Worldline expects to have gained at least a project based on some of the assets produced at M-Sec or related to the value proposition developed within M-Sec.

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:

- The fact that the part of Blockchain can be hosted on the Alastria platform would increase the future accessibility of the solution even after the conclusion of the project.
- Collaboration with the use case 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.

5.2 ICCS

Business objectives in the project

ICCS/NTUA acts as the Technical Coordinator of the project. Regarding its Research and Innovation actions involvement, ICCS/NTUA is involved in the WP3 (with respect to leading the requirements analysis phase and the specification of the M-Sec architecture) and WP4 (leading Task 4.3 and leveraging its extensive experience in cloud security as well as P2P and blockchains implementation).

ICCS' exploitation will be in the context of the institution's strategic plans, which extend in:

- education,
- technology transfer towards the national and European IT,
  promotion of research and enrichment of the Institute's scientific expertise.

Innovation and exploitation possibilities

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 [23].

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, we 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 multi-cultural and highly innovative environment.

5.3 Ayuntamiento Santander

Business objectives in the project

The role of Santander in M-Sec project is to collaborate in the definition of use cases, aligning the project objectives and the needs of the city, facilitate their implementation as pilots in the city and involve real users. Therefore, the city has become a kind of urban laboratory where new technologies and solutions may be tested and validated. In this sense, Santander is mainly involved in the WP2 (co-leading with NTTE Task2.2, regarding definition, setup and citizens involvement in pilots) and WP5 (taking advantage of its extensive experience in regarding dissemination& communication activities).

The main objectives Santander aims to achieve by participating in M-Sec are listed below:

- enrich the current urban laboratory, by deploying new devices, developing new applications and/or services based on a combination of different technologies;
- improve the quality of life of citizens, offering new solutions or improving existing ones and endeavouring to include different segments of the population;
- reinforce the city's international projection as Smart city, strengthening collaborations with consortium partners and attracting not only new opportunities for collaboration in research projects or consortia, but also other economic activities, such as tourism.

Innovation and exploitation possibilities

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, besides, 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.

Nowadays, Santander is an international reference within Smart Cities due to the combination of two elements: the development of different city initiatives which allow managing city services more efficiently together with the active participation in European research projects, such as M-Sec, that have turned the city into a city lab.

Innovation & exploitation during the project (overall plan throughout the whole duration of the project)

The innovation and exploitation possibilities to be explored during the 3 years of the M-Sec project are the following:

- 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. For this reason, different profiles of society are involved, adapting use cases to their technological knowledge. In this sense, the use case 2 which aims to improve the quality of life of elderly people, has been divided into two pilots, differentiating those older people who do not use new technologies for different reasons from those who do use them in their daily lives. Adapting pilots to the target audience is paramount for successful results.
- In addition, the project will help to validate the use of new technologies with the aim of improving the quality of services, evaluating possible improvements to the services currently offered (e.g. the telecare service) as well as being able to offer new services depending on the success of the pilots (e.g. enriched information in one of the city parks).
- Finally, the municipality will make use of the different municipal channels, such as the municipal website and fora which the municipality takes part in, with the aim of promoting the project, with special emphasis on the pilots developed in the city and also cross-border ones, attracting potential users.

Innovation & exploitation after project conclusion

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

- Main results and lessons learnt from different pilots will be integrated in relevant municipal services. For example, pilots developed within use case1 will allow the municipality to decide whether it is feasible to extend the solution offered in Las Llamas park to other parks in the city.
- In addition, the project and its pilots will be promoted in the forums in which the city participates, reinforcing the concept of urban laboratory.

- Finally, maintain contact with pilots' participants, for example, through dedicated face-to-face meetings, consolidating a community of citizens interested in new technologies.

5.4 TST

Business objectives in the project

TST is an SME which acts as the project's technological partner in the Smart City of Santander within 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 will come from:

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

Innovation and exploitation possibilities

TST is an engineering company specialized on custom design for IoT (Internet of Things) products and services. TST support companies to transform their ideas into innovative, profitable and feasible market solutions, with main focus on Smart City, Agri-food and Energy Efficiency business areas [24].

TST is part 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.

TST has a broad experience in both national and international R&D projects, with scope on electronic systems and devices, wireless networks and smart services & applications. It is also an active member of platforms and forums related to IoT and Smart Cities as NetWorld2020, IoT Council, PostScapes and FIWARE.

Innovation & exploitation during the project (overall plan throughout the whole duration of the project)

TST brings its IoT platform and know-how to the project. M-Sec provides TST team the opportunity to take a step forward in what regards the implementation of security features into their developments, as well as perform tests and validation processes in real life scenarios, not just a lab. In addition, the close interaction

with not only EU based partners but also Japanese ones will provide a really valuable feedback to the team, from both the technical and the social and business oriented point of views.

Furthermore, TST will perform the following innovation and exploitation activities along the course of the project:

- Testing and evaluating project pilots, focusing particularly on their technical features and functionalities while keeping an eye on user's involvement and feedback.
- Take advantage of the opportunity to improve competences and skills related to IoT security and Blockchain implementation.
- Promotion of the innovation conducted within the project in the different fora where TST takes part along the course of M-Sec.

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:

- Include the IoT devices developed along the course of the project in the company's portfolio.
- Apply the novel techniques learnt in M-Sec to other IoT developments important for the company.
- Introduce to other Smart Cities not involved in the project the tool to transform their citizens in active stakeholders in the daily city activity and improvement.

5.5 CEA

Business objectives in the project

CEA/Leti is a technological research institute whose role in the project is to strengthen the end-to-end security of data from the Internet of Things. CEA/Leti participates in WP3 on the definition of the architecture and the associated risks. CEA/Leti is also the WP4 leader for the European side regarding the implementation of architecture and countermeasures at all levels to manage risk, with a reinforced contributions on the device, communication and application level. Objectives of CEA/Leti are:

- pursue the development of innovative hardware technologies for the security of the Internet of Things, such as the integration of secure elements on resource-constrained hardware platforms and the efficient integration of security primitives including encryption and authentication,
- facilitate the deployment of connected objects in a complex environment, while maintaining their integrity and developing their usability with stakeholders for service development,
- to test the technologies coming from the laboratories on a representative field of experimentation and to evaluate the value of these technologies compared to the cases of use,
- to enhance CEA's IoT platform sensiNact with security features and validate it in field trials.

Innovation and exploitation possibilities

Leti, a technology research institute at CEA Tech, is a global leader in miniaturization technologies enabling smart, energy-efficient and secure solutions for industry. Founded in 1967, Leti pioneers micro-& nanotechnologies, tailoring differentiating applicative solutions for global companies, SMEs and start-ups. Leti tackles critical challenges in healthcare, energy and digital migration. From sensors to data processing and computing solutions, Leti's multidisciplinary teams deliver solid expertise, leveraging world-class pre-industrialization facilities. With a staff of more than 1,900, a portfolio of 2,700 patents, 91,500 sq. ft. of cleanroom space and a clear IP policy, the institute is based in Grenoble, France, and has offices in Silicon Valley and Tokyo. Leti has launched 60 start-ups and is a member of the Carnot Institutes network [25].

Innovation & exploitation during the project (overall plan throughout the whole duration of the project)

CEA brings its IoT platform and a set of HW & SW security solutions to the project. M-Sec provides the opportunity to the CEA team to improve its competences and know-how in terms of security and validation in field deployments. Besides, having various cities from Europe and Japan provides valuable feedback to the team, not only from the technical point of view, but also non-technical ones such as social acceptance and business modelling.

In addition, CEA will exploit the project results to

- pave the way for the use of certified components for IoT devices and demonstrate their value in novel cryptographic schemes for encryption and authentication
- enabling trusted application prototyping at the platform level by extending Sensinact with end-to-end security
- transfer the knowledge gathered to the relative initiatives such as the Industrial Internet Consortium, OSGi Alliance as well as the Urban Technology Alliance, a smart city related, testbed-oriented consortium, which it is leading with its European and Japanese partners.

Innovation & exploitation after project conclusion

CEA has plans of commercially exploiting the platform with its industrial and city partners. Its market strategy is based on creating smart city ecosystems at national and international levels and accompanying the cities for their digital transformation.

SensiNact (a unified framework to integrate and manage IoT devices, collect their data and enable application development) follows the open source model for its exploitation. The core of the sensiNact platform is being provided as open source, while the tools and libraries for bringing intelligence, as well as the IoT service creation tool, sensiNact Studio, will be value added extensions.

One of the main "pains" that businesses encounter today is the integration effort, time and maintenance of smart city infrastructures. These namely consist of heterogeneous and un-interoperable IoT devices, regulatory systems, social networks, web applications, etc. in addition to the difficulties of integration with the cities' existing information systems. Today, lack of open, no vendor-lock-in platforms and easy-to-use tools are one of the main barriers for the take-off of smart cities. SensiNact enables interoperability among a

larger set of IoT protocols and platforms, which allows gaining considerable time, effort and consequently reducing developments costs and increase time to market of smart city applications.

In addition, the expertise and developments carried out in M-Sec will be exploited to:

- Propose technological transfer to partners for the securitization of their products and infrastructure as a customization to their business case of the M-Sec platform.
- Identify new research challenges regarding cybersecurity of embedded devices, especially in the field of industrial control systems and smart cities, which employs a large number of devices coordinated by multiple actors.
- Promote trust-based service development over the internet of things with the open-source sensiNact platform

5.6 F6S

Business objectives in the project

F6S is the Dissemination and Community Manager of M-Sec in the EU side, leading WP5 of the project. As such, it aims to:

- Coordinate the communication and dissemination activities at project and partner levels,
- Actively promote the project activities,
- Disseminate the project outcomes to the target audiences and attract new stakeholders,
- Support the engagement with the target audiences,
- Organise the M-Sec online contest, and
- Build the M-Sec community.

Innovation and exploitation possibilities

F6S is a UK based entity that has become the largest Start-up/SME community globally with over 1.3 million start-ups/SMEs and 1.7 million entrepreneurs. F6S delivers more than €2 billion every year to start-ups and SMEs with the leading CRM for deal flow, corporate challenges, structured programs, start-up services, corporate partnering, recruiting, government grants and free start-up resources. F6S has also experience in managing and implementing H2020 projects in innovation, SME/start-up growth, market and investment readiness, community building and other more specific areas [26].

Innovation & exploitation during the project (overall plan throughout the whole duration of the project)

F6S will use the project results to provide additional value for its community and build new services/ features that enable the scale up of F6S community, including the F6S IoT Group. It will also bring knowledge of its market place providing benefits to SMEs and start-ups to the M-Sec audiences.

Through the project activities it also aims to support expanding the solutions developed and establishing collaborations which can last after the project with smart cities initiatives and other Horizon 2020 projects in

the fields of Big Data, IoT, Blockchain, etc. Potential connections could be established with Big Data Value Association, Start-up Europe, European Data Incubator, Block.IS, BlockStart, among others.

F6S will also help reaching out to tech start-ups and IoT innovations that are born global, giving further support for them to connect with other international markets. Finally, as WP5 lead, F6S will be supporting 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 capitalize on the developments achieved during the M-Sec project execution:

- Growth in the Japanese market is a relevant component for the exploitation plan. With the engagement in a EU-Japan collaboration project for the first time, F6S gains cultural knowledge and proximity with Japan, which can further allow to communicate easier and more adequately the value of our platform to Japanese companies, municipalities, universities and tech transfer offices (currently with a low participation), and therefore further foster corporate innovation and connections between innovators, researchers, corporates and cities. For this goal, F6S can make use of its corporate challenges service.
- Being the dissemination partner, F6S is not involved in the use cases as the technical partners, therefore it is not contributing to the advance of technology directly within M-Sec scope. Nonetheless, careful attention will be given to the technologies used or developed, to understand if it could adopt them. F6S is particularly interested in exploring blockchain and cybersecurity related solutions. Depending on the technology which could be adopted, and in case there is interest, the F6S tech team would take the lead on the conversion into a marketable service within the platform, contacting directly the M-Sec partner(s) involved.

5.7 NTTE

Business objectives in the project

NTTE acts as Japanese project coordinator, communication facilitator and supervisor for the local government to identify the requirements that must be covered by M-Sec platform.

NTT East, as a leading regional telecommunications company in Japan, and as a member of the NTT Group, the largest telecommunications and ICT provider in Japan, has contributed to the solution of various regional issues. Taking advantage of previous experience participating in smart city projects between Japan and overseas, as a leader of Japanese consortium with various private companies and research institutes, NTTE will demonstrate the management experience cultivated so far, aiming to develop new communication services that utilize blockchain and security.

The main objectives NTTE aims to achieve by participating in M-Sec are:

- Solve social problems and expand as a new business.

- Discover the technological assets available to NTT Group and provide them to the society.
- To start ‘real service’ in several cities with the project partners.
- To expand NTTE Business Portfolio not only in telecommunications being domain but also in the various Connected Social domain.

Innovation and exploitation possibilities

The Nippon Telegraph and Telephone Corporation, commonly known as NTT, is a Japanese telecommunications company headquartered in Tokyo, Japan. NTT is the fourth largest telecommunications company in the world in terms of revenue, as well as the third largest publicly traded company in Japan [27].

NTTE is strongly committed to the notion of corporation as members of society, always strive 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 grow 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 help them to improve network quality, extend telephone services to all areas, and build up their own supply of skilled personnel. In return, NTTE have received numerous commendations and certificates of appreciation from both the assisted nations and the Japanese government.

Innovation & exploitation during the project (overall plan throughout the whole duration of the project)

Contribute to this project by the following technologies and knowledge.

- Effective implementation of field trial and dissemination of M-Sec results leveraging relationship between municipalities and enterprises in various fields
- Closed area network, Cloud service.
- Implementing procedures for quality management.
- Implementing an administration and communication infrastructure to establish a basis for efficient and easy communication within the project.
- Performing a procedure for updating and revising the plans due to changes and new knowledge.

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 build 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 Olympics and Paralympics in Tokyo 2020.
- 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.
- Contributing to the solution of social issues and realization of SDGs, etc. as the NTT Group by implementing the smart city.

5.8 KEIO

Business objectives in the project

KEIO leads WP2 Use cases, Pilots and citizen involvement, integration and validation leveraging its experience on a number of smart city projects and field tests. It is also responsible for Task 3.3, Task 4.5, and Task 5.4, respectively from the aspect of requirement analysis, technology building, and community building. Keio has been involved in the Smart City Project on the efficient development and operation of social infrastructure using ICT. The reason for this participation is the growing need for research on safe and open smart cities in the IoT era. In particular, Fujisawa City, where the university is located, has issues such as the environment and measures against disasters, and participation in the M-Sec project makes sense in terms of utilizing various research and development results so far. It also has the meaning of contributing to the local community.

At the same time, KEIO will make progress in view of sharing information among participating members and sharing of projects beyond WP.

Our objectives are the following:

- To define and describe in full detail the project use cases in such a way that will be the starting point for the further requirements analysis and the M-Sec implementation activities.
- To define the details on how the M-Sec pilots and trials will be set up and organized and to implement the pilots with maximum possible citizen engagement.
- To define an overall integration plan for delivering the M-Sec platform and undertake the necessary integration activities of the various components that will be implemented in the project (under WP4).
- To validate and evaluate M-Sec in terms of technical capabilities, conformance to the initial requirements from the user perspective as well.

Innovation and exploitation possibilities

Keio University was established in 1858 by Yukichi Fukuzawa as a small school of Western learning, Keio has a history as Japan’s very first private institution of higher learning [28]. Keio University has been carried out on technology: (1) urban data collection technology using IoT, etc., (2) urban data distribution promoting

data utilization in various organizations, in order to build a smart city foundation that solves various problems of cities, Research and development and (3) urban data analysis technology that estimates urban conditions based on acquired data. In addition to research and development, verification of research and development results has been conducted through multiple demonstration experiments, and some research results have already been incorporated into administrative services in Fujisawa City, Kanagawa Prefecture, and other efforts have been made to implement social implementation.

Innovation & exploitation during the project (overall plan throughout the whole duration of the project)

- Contribute to this project by the following technologies and knowledges.
    - Deployment of KEIO's technologies and knowhow in the following area
        - Automotive IoT sensing and data analytics
        - Image recognition and automatic object detection
        - Participatory sensing
        - Web sensing
- Serve as a basis for the activities in this project through our following expertise.
    - Data collection: IoT sensing, participatory sensing, utilize open data.
    - Effective data distribution: SOXFire [29] (a multi-community city-wide sensor network for sharing social big sensor data in smart cities) as data distribution platform.
    - Data analytics: Image recognition, deep learning.
- To define an overall integration plan for delivering the M-Sec platform and undertake the necessary integration activities of the various components that will be implemented in the project (under WP4).
- To validate and evaluate M-Sec in terms of technical capabilities, conformance to the initial requirements from the user perspective as well.

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:

- Conduct development on applications and services in various domains, such as industry and government.
- Publish the research outcome from the aforementioned applications and services to well-known top-rank conferences and journals.
- Give feedbacks from applications/services development and conference publications to M-Sec platform.

5.9 NTTDMC

Business objectives in the project

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). Responsible to research the IPR and GDPR 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.

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.

Our specific objectives in the course of this project are the following:

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

Innovation and exploitation possibilities

NTT DATA INSTITUTE OF MANAGEMENT CONSULTING, Inc. has taken it as our mission to enrich society. In keeping with this mission, we 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. We are seeing the rise of business models applying new technologies. Sometimes also demand management adapted to internal and external changes in the social and economic environment, as well as organizational management geared for innovation.

We have constantly polished our skills and capabilities while bolstering our approaches to such environmental changes [30]

Innovation & exploitation during the project (overall plan throughout the whole duration of the project)

- Contribute to this project by the following technologies and knowledges.
    - To create upcoming styles of smart cites
    - To deliver deep insight into the coordination between Japan and EU business model and IPR
- Serve as a basis for the activities in this project through our following expertise.
    - Insight into Japanese smart cities, business model, ICT, regulation and IPR
- To exploit planning activities about smart city models.
- To define IPRs which will be used about smart city models.

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 campus to the smart city business in Japan.

5.10 WU

Business objectives in the project

WU 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 will work on self-adaptation of smart city application to maintain high security levels in response to changes in the environment. WU will also contribute to analysis and design of M-Sec platform architecture.

Based on that background and motives, our objectives are the following:

- To broaden the evaluation in a continuum that will cover 360 degree of the M-Sec ecosystem evaluation.
- To handle both technical and stakeholders evaluation perspectives.
- To leverage in its condition of IoT devices provider to set a series of conditions to get within M-Sec a truly-secured IoT system.

Innovation and exploitation possibilities

Waseda University is a private, independent research university in central Tokyo, Japan, founded in 1882. 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, we have established Institute for Advanced ICT Research in 2018. At this research institute, we will promote research and development on cutting-edge ICT basic technologies that support the future ultra-smart society [31].

Promote research and development of basic technologies such as AI (artificial intelligence), 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 them organically, promoting social implementation through collaboration with different fields such as agriculture, medical care, transportation, and electricity.

Innovation & exploitation during the project (overall plan throughout the whole duration of the project)

- Contribute to this project by the following technologies and knowledges.
  - Provide controller synthesis tool and techniques and automated model learning tools.
  - Apply these techniques/tools to synthesize management policies of the platform to ensure security goals.
  - Our techniques will enable automatic generation of a security management policy with formal guarantees.
- Serve as a basis for the activities in this project through our following expertise.
  - Robot control systems
  - Smart transportation systems.
- To broaden the evaluation in a continuum that will cover 360 degree of the M-Sec ecosystem evaluation.
- To handle both technical and stakeholders evaluation perspectives.

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:

- By building research results in this project on secure and open smart city ICT architecture, we will enhance research on next-generation architecture.
- A secure and flexible IoT architecture will be implemented to realize an architecture that can cope with more complex issues, and apply it to more advanced ICT and smart city relationships in the future.

5.11 YNU

Business objectives in the project

YNU will mainly contribute 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 will work on securing the sensor devices used in the use cases as well as the sensor data.

In M-Sec project, our specific objectives are the following:

- To develop an intrusion detection system (IDS) to be embedded into the sensor devices.
- To define and implement IoT cloud/data security-layer.

Innovation and exploitation possibilities

Yokohama National University is a leading national university located in Yokohama, Kanagawa Prefecture, Japan. Yokohama National University comprises five graduate schools and four undergraduate faculties. Yokohama National University is one of leading national universities in Japan.

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. The institute conducted research from FY2014 to FY2017 as part of its Phase I. The results of this research was well-received, and as a result the aforementioned grant for running the IAS has been approved as a recurring expense beginning in FY2018 [32].

Yokohama National University has many achievements in national projects etc. as a leading research base for information and physical security research and development. In recent years, we are participating 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)".

Innovation & exploitation during the project (overall plan throughout the whole duration of the project)

- Contribute to this project by the following technologies and knowledges.
    - To utilize its state-of-the-art honeypot system for studying attack vectors on IoT devices.
    - To suggest appropriate counter measures for protection.
    - To contribute in the development of secure smart cities and societies.
- Use the following expertise as a basis for the activities in this project:
    - Honeypot based study of attacks for protecting IoT devices.
    - Cloud/data security for IoT devices.
- To develop an intrusion detection system (IDS) to be embedded into the sensor devices.
- Implement IoT device-level security and IoT cloud/data-level security.

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 both at home and abroad by supporting the realization of a secure IoT network and devices from the research and development aspect of this project.
- By clarifying various security issues in the smart city, security risks, and countermeasures for them in this project, we will support future domestic and overseas security measures from research and development.

5.12 NII

Business objectives in the project

As Japan's only general academic research institution seeking to create future value in the new discipline of informatics, the National Institute of Informatics (NII) seeks to advance integrated research and development activities in information-related fields, including networking, software, and content. These activities range from theoretical and methodological work through applications. As an inter-university research institute, NII promotes the creation of a state-of-the-art academic-information infrastructure (the Cyber Science Infrastructure, or CSI) that is essential to research and education within the broader academic community, with a focus on partnerships and other joint efforts with universities and research institutions throughout Japan, as well as industries and civilian organizations [33].

NII is the leader of WP3 “Requirements, architecture, hyper connected smart city” along with its responsibility on Task 3.1 “System level and User level Requirements analysis”, Task 4.2 “P2P level security and blockchains”, and Task 4.3 “Application level security”, given its expertise in dependable and secure software engineering. In particular, NII will work on security and privacy software requirements of smart city application to maintain high security levels. NII will also contribute to analysis and design of M-Sec platform architecture.

Based on that background, MS-Sec project will enhance our opportunities for studying upcoming informatics movement, such as blockchain and IoT. By leveraging those research outcomes, we can support creating future value where security, open network are well balanced.

Our objectives are the following:

- To set out a complete list of requirements which cover both the system and user level to get a
- robust, resilient and sustainable solution.
- To analyse security threats to the M-Sec framework with blockchain.
- To tackle the research challenges and issues that stem from the need to facilitate convergence of IoT security with blockchain to support an innovative smart city platform.

Innovation and exploitation possibilities

The National Institute of Informatics (NII), founded in 2000, is an inter-university research institute corporation and a research organization of information and systems. The mission of 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 artificial intelligence, Big Data, the Internet of Things (IoT), and information security, NII features in a wide range of research activities. We push forward with fundamental research valued from the long-term view as well as practical studies aimed at resolving current social problems [33]

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) [34] science information network.

Innovation & exploitation during the project (overall plan throughout the whole duration of the project)

- Contribute to this project by the following technologies and knowledge.
  - To develop and use Security Analysis Tool
  - To develop valuable Methods for a secure service
- Serve as a basis for the activities in this project through our following expertise.
  - Security requirements
  - Security analysis
- To analyse security threats to the M-Sec framework with blockchain.
- To tackle the research challenges and issues that stem from the need to facilitate convergence of IoT security with blockchains to support an innovative smart city platform.

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:

- By modelling the correct risk analysis for threats, you can see how much cost you need to pay for enhancing security and broaden your research menu.
- By clarifying the criteria for determining whether a system should be covered by a threat or a threat that should be covered by an operation, it is possible to reduce omissions and omissions of security measures, and to establish examination results on the security mode. In addition, development in other fields is also possible.

6. Conclusions and next steps

6.1 Conclusions

The purpose of this task is to plan appropriate activities towards the commercialization of M-Sec results and handle intellectual property rights (IPR) issues. In order to do so, the consortium has conducted a market research and analysis including a state of art of similar initiatives on the market in order to identify M-Sec position in the market, followed by a SWOT analysis to identify barriers and drivers that will help M-Sec on setting the correct strategy to compete successfully.

Additionally, a business model canvas has been developed for each of the use cases along with an individual exploitation plan to be developed by each partner both during and after the conclusion of the project in order to guarantee maximum results in terms of M-Sec exploitation.

Finally, assets already generated before the project have been identified along with its owner and therefore there is not any IPR issue raised by any of the partners. During the upcoming months, the consortium will start to also identify innovation components (those assets to be generated within the length of the project).

This is a summary of the main decisions taken in order to achieve the best use of the funding obtained:

- Regarding M-Sec value proposition, M-Sec will be positioned through the project as a platform able to provide secure, interoperable interactions between IoT elements based on a holistic secured cloud/edge/IoT context within a future smart city. Strengths will be potentially disseminated in order to attract a wider audience and engage stakeholders.
- Sustainability of the platform especially after conclusion of the project will depend strongly on the stakeholder's engagement as they can provide special support on the platform maintenance after finalization. For this, it makes special importance on how M-Sec offers a complete solution, not just a platform but also several components and APIs that help future users to carry out their projects, which is something new in today's market context, an aspect that has an influence over M-Sec's value proposition.
- All partners have initially identified their individual exploitation plan during the length of the project and after the project conclusion. Most of the partners priorities are to improve competence skills; transfer knowledge; develop assets that can be used in other projects or solutions as well as to expand their internal portfolio; strength collaborations among partners for future opportunities and improve quality of life and services with a solution like M-Sec.
- Regarding IPR from assets generated within the project, as WP4 Multi Security layers have just started 2 months ago, the consortium will conduct further IPR management activities and hold discussions related with the components generated within the project life. For assets generated before the project, not issues are raised on this stage as owners for each of the assets have been identified since the very beginning.

- Business Model canvas for each use case have been developed and will be redefined during the next two iteration of this deliverable in order to adjust them appropriately having into account feedback obtained through the implementations of each of the pilots.

6.2 Next steps

This is a first version of the plan, which will need necessarily a future revision, at a later stage of the project (M24 and M36), in order to update the vision of the exploitation plans that we have currently. During the second year of the project, it is expected to have a first prototype of how the M-Sec platform will look and some of the pilots are also planned to start. Therefore, all the feedback gathered from the point of view of users and stakeholders will be considered for the redefinition of the exploitation plan of M-Sec and the sustainability of the platform. In addition, assets to be generated within the project will be identified and analysed in order to approach the best strategy for IPR and avoid any issue concerning property of the assets.

References

[1] https://www.abiresearch.com/market-research/product/1029577-smart-cities-platforms-and-standards/?utm_source=i-scoop

[2] http://www.fiwoo.eu/

[3] https://www.rambus.com/security/cryptomanager-platform/

[4] https://fybr.com/the-fybr-platform/

[5] https://www.iota.org/

[6] https://pr.blonde20.com/iota-taipei/

[7] https://www.newsbtc.com/2018/07/09/iota-ready-to-be-tested-in-eu-funded-smart-city-project/

[8] https://www.waltonchain.org/ct/

[9] https://www.powerledger.io/

[10] https://ec.europa.eu/digital-single-market/en/blogposts/fighting-cybersecurity-eight-new-eu-funded-projects-more-secure-iot

[11] https://seriot-project.eu/

[12] https://secureiot.eu/vision

[13] https://wisdom.nec.com/en/solutions/2019030401/index.htm

[14] https://uhuru.co.jp/en/news/press-releases/20190108-2/

[15] http://www.brain-iot.eu/

[16] https://biotope-project.eu/overview

[17] https://www.decenter-project.eu/

[18] https://iot-analytics.com/state-of-the-iot-update-q1-q2-2018-number-of-iot-devices-now-7b/

[19] https://www.cbronline.com/news/fake-ransomware-sonicwall

[20] http://www.onem2m.org/images/files/oneM2M_WhitePaper_SmartCitiesDoneSmarter.pdf

[21] https://medium.com/seed-digital/how-to-business-model-canvas-explained-ad3676b6fe4a

[22] https://worldline.com/

[23] www.iccs.ntua.gr

[24] http://www.tst-sistemas.es/

[25] http://www.leti-cea.fr/cea-tech/leti/Pages/Accueil.aspx

[26] https://www.f6s.com/

[27] https://www.ntt-east.co.jp/en/

[28] https://www.keio.ac.jp/en/about/

[29] https://keio.pure.elsevier.com/ja/publications/soxfire-a-universal-sensor-network-system-for-sharing-social-big-

[30] https://www.nttdata-strategy.com/english/

[31] https://www.waseda.jp/top/en

[32] https://www.ynu.ac.jp/english/research/

[33] https://www.nii.ac.jp/en/about/

[34] https://www.sinet.ad.jp/en/aboutsinet-en