Multi-layered Security Technologies

for hyper-connected smart cities

D5.7: Market Analysis and Exploitation – 2nd year

June 2020

Grant Agreement No. 814917

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

Project acronym	M-Sec
Deliverable	D5.7 Market Analysis and Exploitation – second year report
Work Package	WP5
Submission date	June 2020
Deliverable lead	WLI/NTTDMC
Authors	WLI, NTTDMC, TST, ICCS, YNU, NII, KEIO, WU, F6S & NTTDMC
Internal reviewer	ICCS/NTTE
Dissemination Level	Public
Type of deliverable	R

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

Version history

#	Date	Authors (Organisation)	Changes
v0.1	3 February 2020	WLI	Table of Contents, Full Draft
v0.2	12 February 2020	NTTDMC	Table of Contents updated
v0.3	22 February 2020	WLI	Sections 5, 6.3, and 7 updated
v0.4	6 May 2020	TST	Section 1.1.1 updated
v0.5	18 May 2020	ICCS	Section 2.1.3 updated
v0.6	20 May 2020	YNU	Section 2.1.2 updated
v0.7	22 May 2020	NTTDMC	Section 3 updated
v0.8	2 June 2020	WLI	Sections 1, 6, 8 and 10 updated
v0.9	9 June 2020	NII, TST	Section 1.1.1 updated
v0.10	10 June 2020	WU, KEIO	Section 2.1.5 updated
v0.11	12 June 2020	NTTDMC	Section 2 and 4 updated
v0.12	15 June 2020	NII	Section 2.1.4 updated
v0.13	17 June 2020	ICCS	Sections 2.1.3, 6, and 7 reviewed
v0.14	17 June 2020	WLI	Review to submit the document for internal review
v0.15	18 June 2020	NTTDMC	Section 3 conclusions updated
v0.16	18 June 2020	YNU	Section 7.1 updated
v0.17	19 June 2020	WLI	Section 7.1 updated, Document reviewed
v0.18	23 June 2020	F6S	Section 9 updated
v0.19	24 June 2020	NTTE	Section 9 updated
v0.20	25 June 2020	F6S	Section 9 updated
V0.21	25 June 2020	ICCS	Internal review
v0.22	29 June 2020	WLI	Addressed review comments
v0.23	29 June 2020	ICCS	Last review comments
V1.0	30 June 2020	WLI	Final version

Table of Contents

List of Tables

List of Figures

Glossary

Acronym	Description	Acronym	Description
AI	Artificial Intelligence	IoTPFs	Internet of Things Platforms
API	Application Programming Interface	IP	Internet Protocol
App	Application	IPR	Intellectual Property Rights
AWS	Amazon Web Services	JP	Japan
B	Billion	M	Million
BPaaS	Business Process as a Service	M*X*	Month X (number)
CAGR	Compound annual growth rate		
		M2M	Machine to Machine
CEF	Connecting Europe Facility	ODS	Operational Device Security
D	Deliverable	PaaS	Platform as a Service
DDoS	Distributed Denial-Of-Service	PCI DSS	Payment Card Industry Data Security Standard
DTLS	Datragram Transport Layer Security	PIPA	Personal Information Protection Act
E2E	End-to-end	SIM	Subscriber Identity Module
EU	Europe	SotA	State of the Art
GDPR	General Data Protection Regulation	SWOT	Strengths, Weaknesses, Opportunities, Threats
HIPPA	Health Insurance Portability and Accountability Act	S2aaS	Sensing-as-a-Service
IaaS	Infrastructure as a Service	T	Task
ICT	Information and Communications Technologies	TLS	Transport Layer Security
ID	Identity Document	TTA	Telecommunications Technology Association
IoT	Internet of Things	WP	Work Package
IDC	International Data Corporation	ZB	Zettabytes

1. Introduction and scope

1.1 Introduction

M-Sec is developing a multi-layer secure IoT framework that is compatible with the transfer and processing of personal data between the EU and Japan. The M-Sec framework provides the technological foundation to comply with GDPR, PIPA, and the Adequacy Agreement between EU&JP, and will be validated through its two cross-border use cases. The goal of this deliverable is to provide a more detailed view of the market possibilities, the M-Sec offering and business models for a solution like M-Sec. The aim is to provide a second draft of the business and exploitation plan to ensure sustainability after the project ends. In particular, the outlined presents the competitors' and stakeholders' analysis, indicating the value proposition of M-Sec by highlighting its core contributions, its advances and its offering and the possible business models to be adopted after the end of project for the M-Sec sustainability.

Thus, Section 2 provides the market drivers for a solution such as M-Sec and the SotA of the current technologies used within the project, indicating how M-Sec contributes to five major challenges from a security point of view.

Sections 3 and 4 focus on platforms/frameworks which provide end-to-end security in the smart city context and on how M-Sec is positioned among them. Additionally, the SWOT analysis already presented on the first version of deliverable Market Analysis and Exploitation (D5.6 Market Analysis and Exploitation-first year) is updated and includes a more technical point of view.

Section 5 identifies the main stakeholders that need to be engaged, assessing their interest and needs and categorising them, according to different levels of engagement; the level of interest and level of influence with the objective to create a communication plan to be included on T5.1 "Dissemination and Communication Activities" and achieve the highest impact possible for the project.

Section 6 defines M-Sec as a Product and presents the M-Sec Business Model and Value Proposition.

Section 7 identifies the M-Sec core system components as well as the pilot system components with a short description on the value provided by each one of them and evaluates different licensing approaches, including a complete list of technologies used in the project with respective licenses and consideration on the licensing decisions for the whole framework.

Section 8 analyses the different revenue models that could be applied to a platform like M-Sec in order to ensure sustainability after the project's conclusion to cover the running costs.

The Marketing plan is presented on Section 9.

Finally, on section 10 conclusions and next steps are exposed.

1.2 Relation to other WPs and Tasks

"Task 5.2 - Exploitation activities" receives input from WP2 and in particular from Tasks "Task 2.1 - Use cases description" and "Task 2.2 - Pilots: definition, setup and citizens involvement" through the corresponding deliverables (D2.1, D2.2 and D2.3).

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

Furthermore, "Task 3.2 - M-Sec Architecture" and the whole "WP4 - Multi Layered Security" contribute to the identification of components generated before and through the project, the value provided by M-Sec as well as IPR issues related.

1.3 Methodology

In order to assess the viability for the M-Sec Project as well as the sustainability to implement a Go to Market Strategy after the project conclusion, the consortium has structured the document in different phases to evaluate the potential of M-Sec.

- **PHASE 1 Market Analysis:** In Section 2, a study and assessment of the market is provided. This is the basis to understand the current market trends and SotA of the technologies employed within M-Sec, and how M-Sec addresses the current challenges. The analysis helps to understand how the market is evolving and how opportunities and threats relate to the M-Sec strengths and weaknesses and what are the Market drivers for a solution such as M-Sec.
- **PHASE 2 Competitor's Analysis:** A study and assessment of the current and potential companies that M-Sec expects to compete with due to covering the same scope. The objective of Competitors' Analysis is to develop a profile of each competitor to help define Strategic Positioning / Competitive Advantage, and lay the foundation for determining the M-Sec value added and positioning in the market (Section 3).
- **PHASE 3 SWOT:** Once the current market is explored and the competitive analysis analysed, the next step is to conduct a SWOT Analysis. Conducting a SWOT analysis will help to understand the internal and external factors to define the value proposition of M-Sec (Section 4).
- **PHASE 4 Stakeholders Analysis:** The next step is to conduct a stakeholder mapping process in order to identify which stakeholders need to be engaged, to achieve the highest impact for the project (Section 5).
- **PHASE 5 Business Model Canvas & Value Proposition:** In section 6, a business model canvas and value proposition for the whole solution provided by M-Sec can be found. This supports the strategy of the business plan to identify for whom the consortium is solving the problem; how we create customer value; how M-Sec will be distributed to stakeholders; how M-Sec will stay competitive; and all revenue and costs that can be anticipated.
- **PHASE 6 Financial Planning & Revenue Models:** The Financial Plan component of the Business Plan is a statement of M-Sec current financial position, its projected financial position over time as the business grows, its strategy for seeking investors, and its Exit Strategy. It is a key part of determining the viability

of the business model, and essential for lenders and investors who want to see hard figures before putting money into your company (Sections 7 and 8).

- **PHASE 7 Marketing Plan:** The Marketing Plan is the tactical plan for taking all of the internal analysis and strategy components of the Business Plan, and turning them into a “plan of action” used to engage the external market of potential customers and partners (Section 9).

Figure 1. Business Plan Methodology

2. Market Analysis

2.1 State of the Art

2.1.1 IoT Security

The popularity of the Internet of Things (IoT) trend continues to see explosive growth, to the point where there will be more than 20 billion IoT devices in place by the end of 2020. The IoT market size in Europe is estimated to reach €242,222M[1] then. IoT devices demonstrate real business value in helping entire industries become more efficient and competitive.

Yet, IoT devices still present one major concern: cybersecurity. This rise in popularity of IoT-connected devices leads to rise in IoT App development does come with its fair share of concerns and security challenges. All in all, traditional security tools and past approaches simply do not work for IoT devices. Even worse, many organisations do not realise just how vulnerable they really are, and may be inadvertently exposing their entire company to threat, such in the case of data breaches, data exfiltration and more.

The largest security challenges currently plaguing the field of IoT-connected devices nowadays are:

1. Insufficient testing and updating. Most of IoT devices and products do not get enough updates while, some do not get updates at all. This leaves trusted customers exposed to potential attacks, as a result of outdated hardware and software. To protect customers against such attacks, each device needs proper testing before being launched into the public, and companies need to update them regularly.
2. Brute-forcing and the issue of default passwords. The Mirai botnet[2], used in some of the largest and most disruptive DDoS attacks is perhaps one of the best examples of the issues that come with shipping devices with default passwords and not telling consumers to change them as soon as they receive them. Weak credentials and login details leave nearly all IoT devices vulnerable to password hacking and brute-forcing in particular.
3. IoT malware and ransomware. While the traditional ransomware relies on encryption to completely lock out users out of different devices and platforms, there is an ongoing hybridisation of both malware and ransomware strains that aims to merge the different types of attack. The ransomware attacks could potentially focus on limiting and/or disabling device functionality and stealing user data at the same time.

---

1 https://books.google.es/books?id=DtbpDwAAQBAJ&pg=PA134&lpg=PA134&dq=The+IoT+market+to+reach+%E2%82%AC242,222&source=bl&ots=DGHjXqK0ji&sig=ACfU3U0a8cWso_sFGIf113NW9XTPJBAbuQ&hl=es&sa=X&ved=2ahUKEwjD1MSU9qjqAhVR5uAKHfD5AgUQ6AEwAHoECAoQAQ#v=onepage&q=The%20IoT%20market%20to%20reach%20%E2%82%AC242%2C222&f=false

2 https://en.wikipedia.org/wiki/Mirai_(malware)

4. IoT botnets aiming at cryptocurrency. While most find blockchain resistant to hacking, the number of attacks in the blockchain sectors seems to be increasing. The main vulnerability is not the blockchain itself, but rather the blockchain app development running on it.
5. Data security and privacy concerns (mobile, web, cloud). Data is constantly being harnessed, transmitted, stored, and processed using a wide array of IoT devices. Commonly, all these user-data are shared between or even sold to various companies, violating users' rights for privacy and Data security and further driving public distrust.
6. Small IoT attacks that evade detection. As important as large-scale attacks can be, there should also be a fear to the small-scale attacks that evade detection. We are guaranteed to see more and more micro-breaches slipping through the security net in the next couple of years.
7. AI and automation. AI tools and automation are already being used to sift through massive amounts of data and could one day help IoT administrators and network security officers enforce data-specific rules and detect anomalous data and traffic patterns. However, using autonomous systems to make autonomous decisions that affect millions of functions across large infrastructures such as healthcare, power and transportation, might be too risky, especially once it is considered that it only takes a single error in the code or a misbehaving algorithm to bring down the entire infrastructure.
8. Home Invasions. Nowadays, IoT devices are used in a large number at homes and offices, something that has given rise to home automation. The security of these IoT devices is a huge matter of concern as an attack can expose users IP addresses that can pinpoint their residential addresses.
9. Remote vehicle access. Smart cars are on the verge of becoming reality with the help of connected IoT devices. However, due to their IoT association, they also possess a greater risk of a car hijack.
10. Untrustworthy communication. There are many IoT devices which send messages to the network without any encryption. This is one of the biggest IoT security challenges which exist out there.

By geography,. In terms of revenue, North America appears to be the dominant market. The growth of this region can be attributed to the extensive deployment of IoT devices across several domains and countries and the enforcement of regulatory frameworks. For example, the implementation of laws such as Payment Card Industry Data Security Standard (PCI DSS) and Health Insurance Portability and Accountability Act (HIPPA) have been propelling the market.

The IoT security market in Asia Pacific has been growing rapidly, thanks to the greater number of business organisations, rise in mobile workforce, and the unregulated usage of the Internet. The expanding economy, social transformation, and the new national security policies in countries such as Japan, India, and Singapore have also been responsible for the growth of IoT security solutions across this region.

IBM Corporation, Symantec Corporation, Infineon Technologies, Cisco Systems, Inc., Hewlett Packard Development Company L.P., Sophos Plc, NSIDE Secure SA, ARM Holdings, Gemalto NV, and Intel Corporation are some of the major companies operating in the global market for IoT security.

IoT security spending was estimated at $703M for 2017 and the fast growing market (CAGR of 44%) is forecasted to reach almost a $4.4B opportunity by 2022, as shown in Figure 2 below.

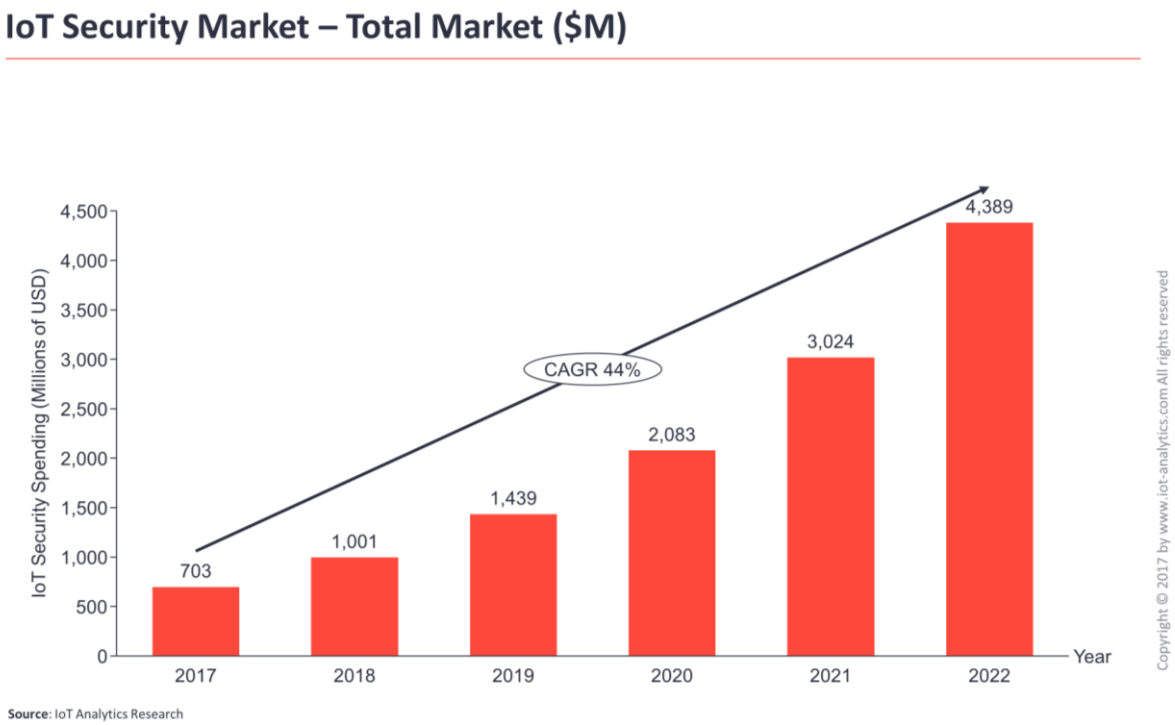

Figure 2. IoT Security Market trend [Source: IoT Analytics Research]

The current situation of the market shows diverse initiatives by smaller companies with the aim in providing a secure IoT. One of these is the one presented by Monogoto[3] which, through its SIM cards, provides worldwide IoT and M2M connectivity, allowing full visibility, event management and control from the network to the edge devices.

One of the goals in M-Sec addresses IoT security and hereby there is a sample on how the project deals with this topic. On the one hand, to protect their customers against brute forcing attacks, each IoT device will go through proper testing before being launched into the public and partners in charge will update them regularly. On the other hand, when dealing with IoT botnets aiming at cryptocurrency, M-Sec IoT applications, structures, and platforms relying on blockchain technology will need to become regulated and constantly monitored and updated to prevent any future cryptocurrency exploits.

However, by placing the focus on the IoT devices themselves, M-Sec will deal with their securitisation, taking into account the following measures:

- **Incorporate security at the design phase.** IoT developers in the consortium include security at the start of any device development, in this case having in mind the envisioned pilots and the potential future exploitation. Enabling security by default is critical, as well as providing the most recent operating systems and using secure hardware.
- **Device identity management.** Providing each device with a unique identifier is critical to understanding what the device is, how it behaves, which are the other devices it interacts with, and the proper security measures that should be taken for that specific device.

[3] https://monogoto.io/

- **Hardware security.** Endpoint hardening includes making devices tamper-proof or tamper-evident. This is especially important when devices are used in harsh environments or where they are not monitored physically.
- **Security gateways.** Acting as an intermediary between IoT devices and the network, security gateways have more processing power, memory and capabilities than the IoT devices themselves, which provides them the ability to implement features such as firewalls to ensure hackers cannot access the IoT devices they connect.
- **Patch management/continuous software updates.** Providing means of updating devices and software either over network connections or through automation is critical. Having a coordinated disclosure of vulnerabilities is also important to updating devices as soon as possible. Consider end-of-life strategies as well.

Regarding data security and privacy concerns M-Sec sets dedicated compliance and privacy rules that redact and anonymize sensitive data before storing and disassociating IoT data payloads from information that can be used to personally identify users. In addition, with regard to the data stored, there is a compliance with various legal and regulatory structures. The same practice is employed with mobile, web and cloud applications and services used to access, manage and process data associated with M-Sec IoT devices.

Finally, to deal with untrustworthy communication and avoid this threat, the best way to do is to use transport encryption and standards like TLS. Another way is to use different networks that isolate different devices, therefore M-Sec can foster the use of private communication which ensures that the data transmitted is secure and confidential.

2.1.2 Cloud and Data Level Security

The digital growth has created a big bang for the digital economy by opening up unlimited opportunities. However, the opportunities are not limited to good guys. Cyber-attacks and data breaches have increased as well, and hackers are reaping an equal amount of profit from this digital growth. Even though the cloud computing is over a decade old, cloud security is still evolving. Data protection has often been a major challenge in information technology. Some of the prominent players in the Cloud security market are: Cisco, IBM, Symantec, Trend Micro, Microsoft, Intel, etc.

According to the GeekWire and Gartner, the cloud computing market will grow from a $153.5B market of 2017 to over $302B by 2021, as shown in the table below.

Table 1 Worldwide Public Cloud Service Revenue Forecast (Billions of U.S. Dollars)

	2017	2018	2019	2020	2021
Cloud Business Process Services (BPaaS)	42.6	46.4	50.1	54.1	58.4
Cloud Application Infrastructure Services (PaaS)	11.9	15.0	18.6	22.7	27.3
Cloud Application Services (SaaS)	60.2	73.6	87.2	101.9	117.1
Cloud Management and Security Services	8.7	10.5	12.3	14.1	16.1

Cloud System Infrastructure Services (IaaS)	30.0	40.8	52.9	67.4	83.5
Total Market	**153.5**	**186.4**	**221.1**	**260.2**	**302.5**

Source: Gartner (April 2017) Note: Totals may not add up due to rounding

Gartner sees double digit growth in cloud adoption, with spending forecast to grow on average 17.1% per year. According to another study done by "Market Research Future" though, the increase in the number of attacks is fuelling the growth of cloud security market worldwide, i.e. from 5B in 2015 to 13B USD growth in 2022.

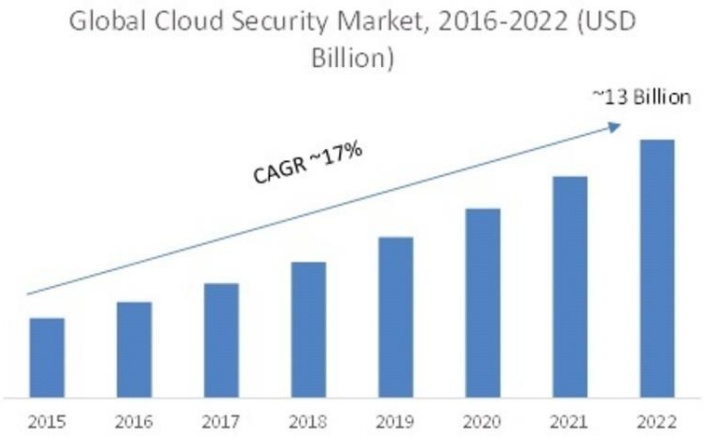

Figure 3. Global Cloud Security Market [Source: Garner]

However, increasing number of reported breaches and the fear of losing data are among some factors limiting the market growth. It has also been noticed that many users have no insight into how their data are being protected by the cloud vendors. According to "Identity Force" (a market leader in identity theft protection provider), 7.9 billion data records were exposed in the first nine months of 2019. Cloud outages from major players like Amazon Web Services (AWS), Apple iCloud, Microsoft Azure, Salesforce, Google cloud, etc. shook market confidence. Therefore, the user's prime concerns are the data security and privacy protection relevant to both hardware and software when it comes to the cloud technology.

M-Sec is addressing the above-mentioned challenges by enabling security-by-design via proven technologies to secure the exchange between data from IoT devices to remote distributed entity in the cloud. The data security methods rely on both software and hardware technologies for providing confidentiality, integrity, availability, and privacy. Strong authentication and encryption is designed to take into account data traversing through the cloud and getting exposed to cyber-attacks. In order to stay vigilant, cyber threats are monitored and the availability of data is ensured by enabling quicker responses. A privacy management tool helps in enforcing GDPR/PIPA compliance on video images by removing sensitive data. Hence, the M-Sec developed solution enhances the security of data between the devices and their respective back-ends in complementary ways.

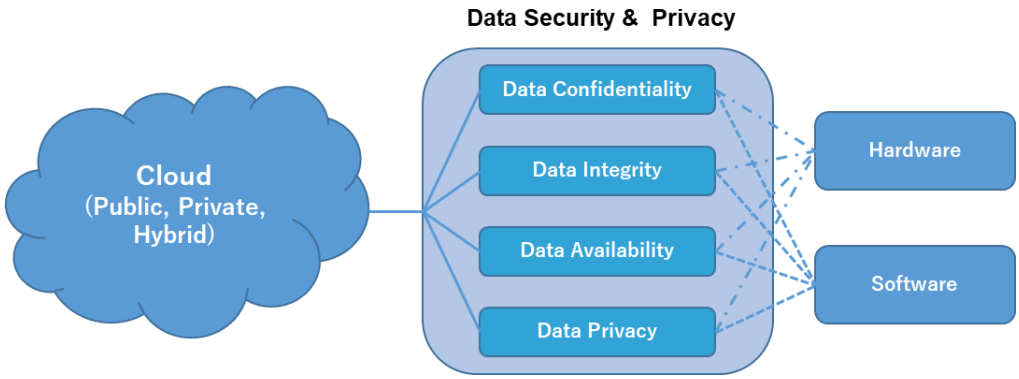

Figure 4 – Cloud and Data Level Security and Privacy

2.1.3 P2P Level Security and Blockchain

During the last years, different solutions have been proposed in the convergence of IoT and Blockchain[13]. However, Internet of Things (IoT) security and privacy remain a major challenge[14]. In this section we present different approaches and platforms based on Blockchain technology and IoT and compare them with M-Sec platform mainly in terms of preserving security and privacy.

- **Sensing-as-a-Service (S2aaS) business model:** A presentation of how blockchain technology could disrupt concepts such as IoT and Sensing-as-a-Service (S2aaS) concepts is given in the work of Noyen et al[15]. S2aaS is a relatively new business model, which brings new data-monetisation opportunities to operators by enabling them to easily sell sensor data. S2aaS makes IoT sensor data more easily accessible to customers, because it allows them to simply access (buy) data from sensors that are already in operation, so they are not obliged to maintain and operate numerous APIs and complex software infrastructures[16]. S2aaS is a promising candidate for an IoT-enabled business model pattern, the same way E-Commerce was a business model for the first wave of the Internet. Besides the introduction to the concept of S2aaS, a description of the characteristics of Blockchain that are relevant for S2aaS applications is provided, such as decentralization, openness, pseudonymous identification, low fees and friction, scriptability and cryptographic verifiability. An extension of this work is presented in the work of Worner et al[17]. While in the former paper the concept of how blockchain technology could disrupt Sensing-as-a-Service was mainly presented on a theoretical basis, in the current paper a working prototype is also presented.

[13] K. Christidis and M. Devetsikiotis, "Blockchains and Smart Contracts for the Internet of Things," IEEE Access, vol. 4, pp. 2292-2303, 2016

[14] Dorri, A., Kanhere, S.S., Jurdak, R. and Gauravaram, P., 2017, March. Blockchain for IoT security and privacy: The case study of a smart home. In 2017 IEEE international conference on pervasive computing and communications workshops (PerCom workshops) (pp. 618-623). IEEE.

[15] K. Noyen, D. Volland, D. Wörner and E. Fleisch, "When Money Learns to Fly: Towards Sensing as a Service Applications Using Bitcoin," 20 9 2014. [Online]. Available: https://arxiv.org/abs/1409.5841. [Accessed 28 6 2018].

[16] Papadodimas, G., et al. (2018, November). Implementation of smart contracts for blockchain based IoT applications. In 2018 9th International Conference on the Network of the Future (NOF) (pp. 60-67). IEEE.

[17] D. Wörner and T. v. Bomhard, "When your sensor earns money: exchanging data for cash with Bitcoin," in 2014 ACM International Joint Conference on Pervasive and Ubiquitous Computing: Adjunct Publication, New York, 2014.

Afterwards, the basic concept of the combination among Bitcoin and S2aaS is presented, by connecting every sensor to the Bitcoin's blockchain and having a unique Bitcoin address. A simple transaction includes three parts, the requester, who has a Bitcoin address, the Bitcoin blockchain and the sensor which also has a Bitcoin address. The requester sends a payment to the Bitcoin address of the sensor through a Bitcoin transaction. When the sensor notices the receipt of the payment, it creates a transaction to the Bitcoin address of the requester, including its most current datum encrypted with the requester's public key. Then the requester decrypts the datum with his private key. However, in most cases (e.g. real-time data feed etc.) S2aaS applications will probably involve the transfer of more than one datum, which makes the process more complex. This problem is solvable now in our M-Sec Marketplace, with the technology of smart contracts that run on blockchains.

  - The M-Sec IoT Marketplace is based on smart contracts and leverages security characteristics of the blockchain technology. We chose to utilize the blockchain technology, in order to let users transact on a P2P level using application specific tokens rather than transacting with a central authority using fiat currency, as would happen if a typical client-server architecture had been chosen. Quorum (Ethereum based) blockchain platform was preferred for the development of this platform because of the security and flexibility it offers, the completeness and maturity of the available development tools and the fact that it is the most popular blockchain platform supporting smart contracts. Additionally, it is supported by a vibrant community that helps it constantly improve and its applications are very easily accessible by potential users[18]. These characteristics provide to Quorum and Ethereum, an advantage over other blockchain platforms, such as EOS, Cardano, Stellar, NEO, that support smart contracts. The developed platform for sharing IoT/application specific data uses a currency (M-sec Token) developed for this purpose. By the use of the M-Sec blockchain framework and the associated smart contracts the M-Sec overall solution will be equipped with features that increase the trust between participating entities and the integrity of data. Additionally, identity verification mechanisms will be applied for increasing the transparency and non-repudiation features of the applications which transact over the M-Sec blockchain.

- **IoTA: The authors of "The Tangle"**[19] proposed a new ledger-based cryptocurrency called IoTA. By eliminating the notion of blocks and mining, IoTA ensures that the transactions are free and verification is fast. The key innovation behind IoTA is the"tangle", which is essentially a directed acyclic graph (DAG). Before a user can send a transaction, he has to verify two randomly chosen transactions generated by other users. As the number of nodes increase, the transactions generated also increase but so do the number of transactions that are verified[20]. However, M-Sec employs a permissioned blockchain unlike the DAG employed by IoTA, thus benefits from the inherent benefits of a blockchain such as the auditability offered by an immutable ledger.
- Hashemi et al.[21] proposed **a blockchain-based multi-tier architecture** to share data from IoT devices with organisations and people. The proposed architecture has three main components namely: data

[18] B. Garner, "Off to the Races: Creating the Best Dapps Platform (Ethereum, NEO, QTUM, Lisk, Cardano)," 30 1 2018. [Online]. Available: https://coincentral.com/best-dapps-platform/

[19] S. Popov, "The tangle," cit. on, p. 131, 2016.

[20] Dorri, A., Kanhere, S.S., Jurdak, R. and Gauravaram, P., 2017. Lsb: A lightweight scalable blockchain for iot security and privacy. arXiv preprint arXiv:1712.02969.

[21] S. H. Hashemi, F. Faghri, P. Rausch, and R. H. Campbell, "World of empowered iot users," in 2016 IEEE First International Conference on Internet-of-Things Design and Implementation (IoTDI). IEEE, 2016, pp. 13–24.

management protocol, data store system, and message service. The data management protocol provides a framework for data owner, requester, or data source to communicate with each other. The messaging system is used to increase the network scalability based on a publish/subscribe model. Finally, the data store system uses a BC for storing data privately. In our approach we do not store data in the blockchain as this would compromise the scalability of our framework but rather focus on the storage of hashes of data in the blockchain.

2.1.4 Application Level Security

Various organisations and groups have published guidelines on IoT Application security. We introduce below the main IoT-related guidelines published by OWASP, NIST and GSMA.

- **OWASP:** The Open Web Application Security Project (OWASP) is an open community dedicated to enabling organisations to develop, purchase, and maintain applications and APIs that can be trusted. The OWASP Internet of Things Project is designed to help manufacturers, developers, and consumers better understand the security issues associated with the Internet of Things, and to enable users in any context to make better security decisions when building, deploying, or assessing IoT technologies.
  - OWSP Internet of Things (IoT) Top 10: OWASP IoT Top 10 represents the top ten things to avoid when building, deploying, or managing IoT systems. The primary theme for the 2018 OWASP Internet of Things Top 10 is simplicity. Rather than having separate lists for risks vs. threats vs. vulnerabilities—or for developers vs. enterprises vs. consumers—the project team elected to have a single, unified list that captures the top things to avoid when dealing with IoT Security.
  - Top 10 Web Application Security Risks: OWASP Top 10 Web Application Security Risks is a standard awareness document for developers and web application security. It represents a broad consensus about the most critical security risks to web applications.
- **NIST:** The National Institute of Standards and Technology (NIST) is part of the U.S. Department of Commerce. NIST is one of the oldest physical science laboratories in US.
  - NIST Special Publication(SP) 800-183: Networks of 'Things': NIST SP 800-183 provides the basic building blocks for a Network of 'Things' (NoT), including the Internet of Things (IoT). This document offers an underlying and foundational understanding of IoT based on the realization that IoT involves sensing, computing, communication, and actuation. The material presented here is generic to all distributed systems that employ IoT technologies.
  - NIST Interagency Report(IR) 8200: Status of International Cybersecurity Standardisation for the Internet of Things (IoT): NISTIR 8200 is developed to explore the current state of international cybersecurity standards development for IoT. The intended audience is both the government and the public. The purpose is to inform and enable policymakers, managers, and standards participants as they seek timely development of and use of cybersecurity standards in IoT components, systems, and services.
- **GSMA** GSM Association (GSMA) represents the interests of mobile operators worldwide, uniting more than 750 operators with almost 400 companies in the broader mobile ecosystem, including handset and device makers, software companies, equipment providers and internet companies, as well as organisations in adjacent industry sectors. GSMA promotes best practice for the secure design,

development and deployment of IoT services, and providing a mechanism to evaluate security measures.

- GSMA IoT Security Guidelines: GSMA IoT Security Guidelines help create a secure IoT market with trusted, reliable services that can scale as the market grows. They Includes 85 detailed recommendations for the secure design, development and deployment of IoT services, addresses security challenges, attack models and risk assessments and provides several worked examples
- ・GSMA IoT Security Assessment: GSMA IoT Security Assessment Is based on a structured approach and concise security controls, covers the whole ecosystem and provides a flexible framework that addresses the diversity of the IoT market.

M-Sec Application level Security

The main focus of M-Sec application level security is to establish engineering foundations to support development of secure smart city applications on the top of M-Sec. Security requirements for smart city applications should be elicited by identifying security goals, components to be protected, and threats. In addition, protection mechanisms mitigating the threats should be designed and implemented in applications according to the previous guidelines. M-Sec provides methodologies and tools to develop smart city applications in order to support developers of smart city applications. The consortium proposes a framework for building a body of knowledge and a knowledge base for secure software development. This framework provides security requirements modelling support system (Security analysis tool) and a Modal System Transition Analyser to eliminate both human errors in designing the application logic and a wide number of tests performed to verify the security level.

2.1.5 Overall End to End Security

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 issues on privacy and data protection. The smart city application is inherently multi-layered including edge, cloud and application layers. The security and privacy issues should be addressed in the all layers to ensure “end-to-end security and privacy”. However, one of the main challenges is to provide end-to-end security in the whole IoT ecosystem, since there are too many parties involved on the IoT application provided (from IoT vendors to cloud and application providers). Lately, there have been new solutions coming to the market that offer an end-to-end approach by establishing major partnerships with different players specialized on different IoT layers.

Within this context, M-Sec provides different components developed on each of the layers to provide the security needed and additionally, a Security Management Tool ensuring a secured and smooth interoperation of each of the elements of the architecture. The Security Management Tool provides a directory service containing all information to manage security services for clients, such services known as AAA for Authentication, Accounting and Authorization.

2.2 Market Drivers

2.2.1 Increased Use of IoT[22]

In addition to conventional internet connected terminals, such as personal computers and smartphones, various things around the world, such as home appliances, automobiles, buildings and factories, are connected to the internet, and the number has exploded. According to a new forecast from International Data Corporation (IDC), the number of devices connected to the Internet, including the machines, sensors, and cameras that make up the Internet of Things (IoT), continues to grow at a steady pace. It is estimated that there will be 41.6 billion connected IoT devices, or "things," generating 79.4 zettabytes (ZB) of data in 2025[23].

By installing sensors and processors that process communication functions and information, new value will be added. A variety of applications are being considered, such as health management using wearable devices, and maintenance and management using sensors in places where it is difficult for human eyes to work or work. First of all, the number of “consumers” and “communication” that proceeds is large at more than 5 billion, and the annual growth rate is expected to be around 10%. In particular, "consumers" are approaching the scale of the world's population of approximately 7 billion.

As one of the drivers of the growth of IoT, “industrial applications” have grown significantly with the spread of so-called M2M, and the number of devices has already reached 3 billion, which is one of the applications that will continue to expand.

2.2.2 New Regulations & Policies[24]

In Japan, based on “The Every-Three-Year Review” provisions, Article 12 of the Supplementary Provisions of the 2015 Amendment Act, the PPC, Personal Information Protection Commission, has engaged in activities to understand actual circumstances and to overview current issues through interviewing experts and relevant organisations. From the perspectives of raised awareness about own personal information, the balance between protection and utilisation, and taking into consideration the technological innovation and necessity to deal with emerging risks due to increased cross border data flow, etc., the following measures will be taken by the amendment of the APPI, Act on the Protection of Personal Information.

- requirements for the cease of utilisation, etc. will be eased in cases in which there is a possibility of violating individual rights or legitimate interests
- Making it mandatory to report to the PPC and to notify a principal
- "Pseudonymously Processed Information" will be introduced
- Penalty will be reinforced

[23] https://www.idc.com/getdoc.jsp?containerId=prUS45213219
[24] https://www.ppc.go.jp/files/pdf/amendment_bill202003.pdf

In the EU, the General Data Protection Regulation (GDPR) came into effect on May 25, 2018. The European Union Charter for Basic Rights, which defines the rights of EU citizens, states that the protection of personal data is a basic human right, and was enacted from the perspective of strengthening this right in the digital age. The GDPR regulates the protection of personal data and privacy more strictly than the EU Data Protection Directive, and has a significant impact on the business development of digital platformers.

There are mainly four points. Firstly, there is the extraterritorial application of the law. In other words, even if the act is from outside the EU, it will be applied when providing goods/services to individuals within the region and collecting personal data. The second point is that it is possible to impose high fines. The third point is that clear consent of the individual is required when collecting and using personal data. And the fourth point is that the rights regarding individual data portability are specified.

2.2.3 High number of Ransomware Attacks[25]

Combatting cybersecurity risks has grown in importance with the evolution of the digital economy. The World Economic Forum published The Global Risks Report 2019 in January 2019. The report identifies, as global risks, large-scale phenomena with the potential to cause large-scale damage worldwide in the next 10 years. The report organizes these risks by their potential likelihood, their impact, and their interconnections.

According to the report, among the global risks that affect multiple domains, (such as economics, society, environment, and technology) cyber-attacks, critical information infrastructure breakdowns, data fraud or theft, and security threats are ranked among the highest in likelihood and impact.

Examining the interconnections among risks shows that cyber-attacks are related not only to data fraud and critical information infrastructure breakdowns, but also to profound social instability, interstate conflict, and failure of national governance

Cybersecurity vulnerabilities and impacts are anticipated to spill out of cyber spaces and affect the real world, as the IoT becomes more prevalent. The IoT and related matters have been moving up in the ranks of cybersecurity trends mentioned above. The NICTER Analysis Report 2018, released by the National Institute of Information and Communications Technology (NICT) in February 2019, listed the top 10 Technology Advancement destination port numbers targeted in major cyber-attacks measures by NICTER. Eight of the 10 ports were associated with IoT devices such as web cameras and home routers. Even the category of Other Ports contains many ports used by IoT devices, such as ports used by online management interfaces for equipment and machines. Therefore, addressing IoT device vulnerabilities has become increasingly important, as IoT turns into a new platform for cybersecurity threats.

2.2.4 Technology Advancements[26]

With the spread of the Internet, cloud, and mobile devices, as well as the development of self-driving cars and smart devices, next-generation technologies such as AI, IoT, Big Data, and blockchains will be used not

[25] https://www.soumu.go.jp/johotsusintokei/whitepaper/eng/WP2019/chapter-1.pdf#page=9
[26] https://innovation.mufg.jp/detail/id=332

only in the technology industry but also in society. It is rapidly gaining attention as it has the potential to transform.

Among them, the reason why interest in thefour major innovation technologies (mentioned above), is increasing is that they can create “synergistic effects” on an unprecedented scale by fusing each other or with other technologies.

The IoT already offers many companies the opportunity to offer new services and products. The vast amount of data obtained from billions of connected devices is used to improve AI applications, and blockchain technology enables IoT information protection and smart contracts. Indeed, the democratisation of technology and the formation of a community that can connect to it will become a reality.

In the future, the “three major innovations” will evolve further, and along with next-generation technologies such as Big Data, 3D printing, 5G (fifth generation mobile communication systems), augmented reality (AR), and quantum computers, automation and digitization have been achieved. There is a very high possibility of pushing it up to a dimension that is not in the market.

Transparency, invariance, low cost, information sharing, efficiency, etc., which were difficult to establish for various reasons using conventional business models, become “common sense in business” and work style reform The basis of the business model including it must be reborn into a completely new one.

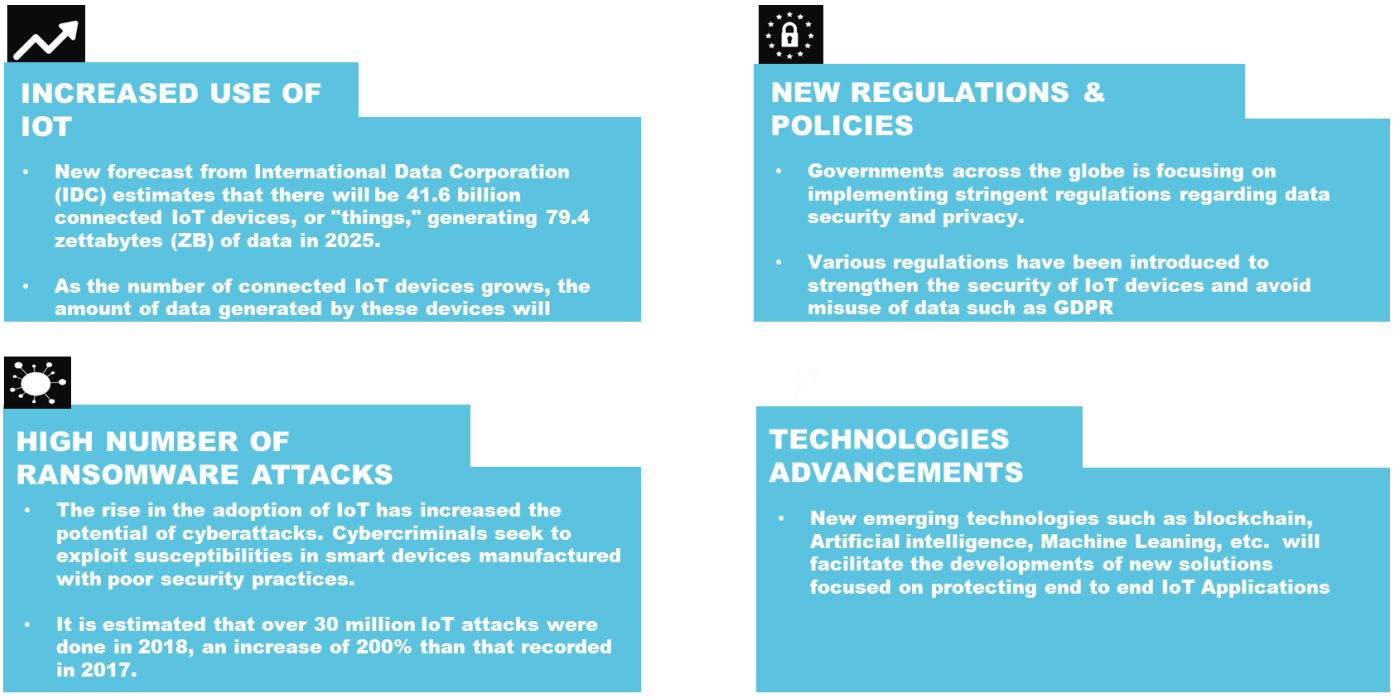

Figure 5. Market Drivers for IoT Security

3. Competitors' Analysis

3.1 Competitors' analysis Methodology

To conduct the competitor's analysis, the consortium has listed the major competitors per different segment of IoT Platforms. The segments are as follows:

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

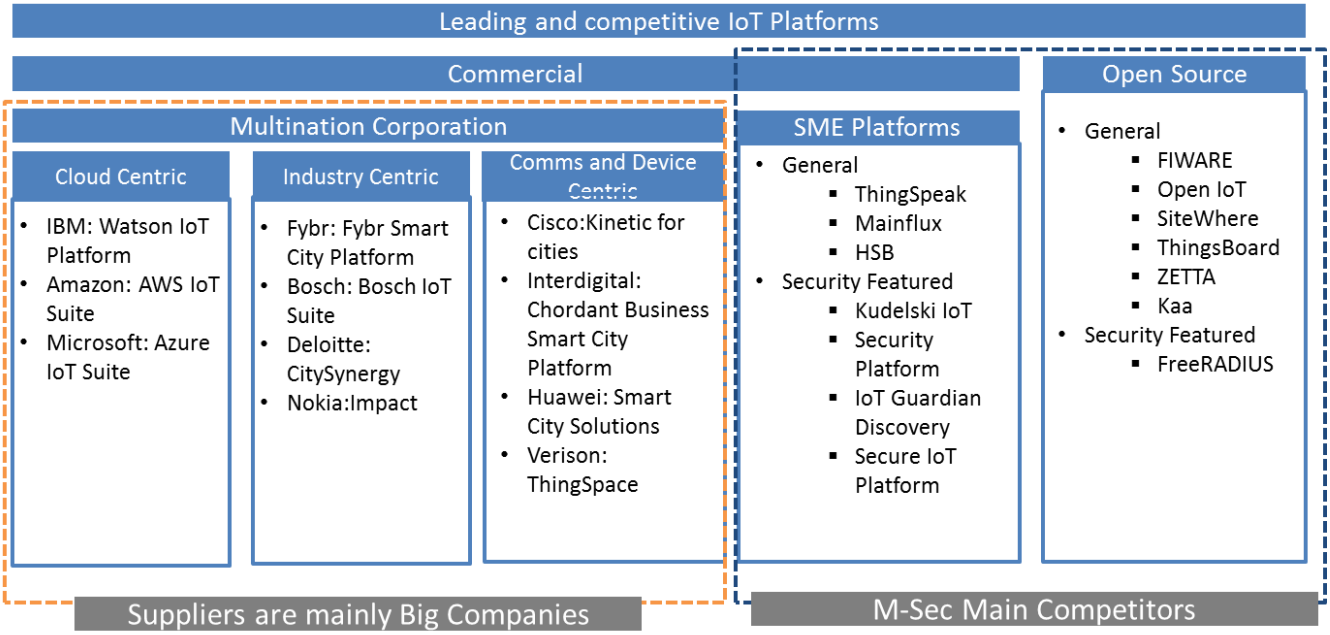

Figure 6. Main competitors per layer and company size

For the competitor's analysis, the consortium has decided to focus on SMEs and open-source software segments that are particularly competitive compared to the characteristics of the M-Sec project, and from these segments, competitive products are investigated. Among the above segments, we are investigating the products that are characterised by the security function that is the feature of the M-Sec project, and are also investigating the representative products in the general-purpose product group.

- SME platforms: It can be further divided into the following two categories.
  - General: Generic products
  - Security featured
- Open Source: It can be further divided into the following two categories.
  - General: Generic products

- Security featured

Also, the products of large companies are not included in the detailed competitive survey because they have different views from the M-Sec project in terms of multi-functionality and promotion and distributors.

3.2 Analysis Results: Main competitors

3.2.1 Secure IoT Platform[27]

- Description
  - Promote security standardisation initiatives that include everything, from the manufacturing stage of IoT devices to services in the cloud environment, through open innovation gathering the knowledge of Japanese industry
- Customer Segment
  - IoT in general
- Target User
  - Japanese ICT system vendors and device makers
- Product Characteristics
  - By securely storing electronic authentication information from the manufacturing stage of IoT devices and linking it with the authentication system, it is possible to provide cloud services only to devices whose existence has been confirmed
  - A mechanism that allows update software to be safely delivered and managed until the end of use
- Distribution Channel
  - Web and distribution with Hardware Partners
- Security Characteristics
  - Three subcommittees have been set up within the Technical/Standardisation Committee to work on the organisation of risks in IoT security and the creation of IoT security guidelines.
  - Will be organized by introduction layer (device manufacturing layer/network layer/data management layer/service layer)/industry/device usage
- Business Model
  - Output of their activities will be used for free by their members. They will create their own business model
- Pricing
  - Not Available
- Strengths
  - IoT security standards that can be used for Japanese IoT market
  - Participation of some major security vendors
  - Case studies will be shared among members
  - PR activities
- Weaknesses
  - Activities are based on research not actual business

[27] https://www.secureiotplatform.org/

- Focused only in Japan

3.2.2 IoT Guardian Discovery[28]

- Description
  - AI-powered, cloud-based platform that detects, identifies, secures, and provides insights into IoT devices.
- Customer Segment
  - Enterprise, healthcare and smart city
- Target User
  - Network managers and smart-city infrastructure management sectors
- Product Characteristics
  - Managing the complex IoT lifecycle is a new challenge for organisations. Automated orchestration by Zingbox IoT Guardian enables you to meet the challenge and extend IT best practices to IoT devices.
  - Five elements: Identify Onboard Secure Manage and Optimize
- Distribution Channel
  - Partnering with global major ICT companies, such as Cisco and VMWare
- Security Characteristics
  - Its Security Operations Center (SOC) dashboard extends SOC processes to monitor IoT devices across multiple sites via a single pane of glass view.
- Business Model
  - Zingbox can get license fee from using this platform. There are a lot of optional services and functions.
- Pricing
  - Not Available
- Strengths
  - AI based security
  - Major partners
  - Security Operation Center support security management
  - Dashboard has good usability
  - Real time situational awareness
- Weaknesses
  - Smart city is just one of its usage, therefore it has not unique smart-city-based characteristics

3.2.3 Kudelski IoT Security Platform[29]

- Description

[28] https://www.zingbox.com/iot-guardian/
[29] https://www.kudelski-iot.com/

- Industry-specific solutions secure the IoT use cases and applications that will transform your business. design trust & control into your IoT products and ecosystem from the start

- Customer Segment
  - Industrial Energy, Telecom, Medical、Automotive, Smart cites
- Target User
  - IoT system and service providers
- Product Characteristics
  - offer products and services for customers at any phase of their IoT development lifecycle. From securing one specific use case to comprehensive support during every step of your IoT design, implementation and operation.
  - integrate security and connectivity as simply as possible in your device
- Distribution Channel
  - unclarified
- Security Characteristics
  - There are many major distributing partners. Some are the leading public cloud providers, such as AWS and Microsoft
- Business Model
  - License fee from using this platform.
- Pricing
  - Not Available
- Strengths
  - Partnership with major public cloud providers
  - Device management
  - Involvement in design phase of IoT devices
  - Support client's business model
  - Lifecycle support of IoT devices
- Weaknesses
  - Smart city is just one of its usage, therefore it has not unique smart-city-based characteristics

3.2.4 Mainflux[30]

- Description
  - Open-source IoT platform with the complete full-scale capabilities for development of Internet of Things solutions, IoT applications and smart connected products. Enhanced and fine-grained security via deployment-ready Mainflux Authentication and Authorization Server with Access Control scheme based on customizable API keys and scoped JWT. Mutual TLS Authentication (mTLS) using X.509 Certificates. NGINX reverse proxy for security, load-balancing and termination of TLS and DTLS connections.
- Customer Segment

[30]MAINFLUX LABS;https://www.mainflux.com/

- City Domain
- Target User
  - Municipality & Enterprise
- Product Characteristics
  - Enhanced and fine-grained security via deployment-ready Mainflux
  - Authentication and Authorization Server with Access Control scheme based on customizable API keys and scoped JWT.
  - Mutual TLS Authentication (mTLS) using X.509 Certificates.
- Distribution Channel
  - Web and distribution with Hardware Partners
- Security Characteristics
  - NGINX reverse proxy for security, load-balancing and termination of TLS and DTLS connections.
- Business Model
  - Free
- Pricing
  - Free
- Strengths
  - Built as a set of microservices containerized by Docker and orchestrated with Kubernetes, Mainflux IoT platform serves as a software infrastructure and middleware which provides:
    - Device management
    - Data aggregation and data management
    - Connectivity and message routing
    - Event management
    - Core analytics
    - User Interfaced
    - Application enablement
- Weaknesses
  - Insufficient way to earn money. They intend to do through consultation service.

3.2.5 FreeRADIUS[31]

- Description
  - FreeRADIUS project, the open source implementation of RADIUS, an IETF protocol for AAA (Authorization, Authentication, and Accounting).
  - the project has grown to include support for more authentication types than any other open source server. It is used daily by 100 million people to access the Internet.
- Customer Segment
  - It is one of OSS protocol not focused in some specific segment
- Target User
  - Used by huge amount OSS software developers. It is used for digital authentication

[31] https://freeradius.org/

- Product Characteristics
  - Used for authentication of wireless LAN and VPN devices
  - FreeRADIUS is used in various Linux distributions such as RedHat Enterprise Linux/CentOS, SuSE Linux Enterprise Server, Debian, and Ubuntu, and can be installed from a package. You can also get long-term support with commercial distributions such as RedHat Enterprise Linux.
- Distribution Channel
  - Major OSS distributers, such as RedHat, are involved in its distribution
- Security Characteristics
  - Used for authentication software of wireless LAN and VPN devices
- Business Model
  - Free
- Pricing
  - Free
- Strengths
  - Digital authentication
  - Long history of its safety
  - 100 million users
- Weaknesses
  - Covering just small part of IoT security platform and function.

3.2.6 FIWARE[32]

- Description
  - The FIWARE Community is an independent Open Community whose members are committed to materialize the FIWARE mission, that is: “to build an open sustainable ecosystem around public, royalty-free and implementation-driven software platform standards that will ease the development of new Smart Applications in multiple sectors”. The FIWARE Community is not only formed by contributors to the technology (the FIWARE platform) but also those who contribute in building the FIWARE ecosystem and making it sustainable over time. As such, individuals and organisations committing relevant resources in FIWARE Lab activities or activities of the FIWARE Accelerator, FIWARE Mundus or FIWARE iHubs programmes are also considered members of the FIWARE community.
- Customer Segment
  - City Domain
- Target User
  - Municipality & Enterprise
- Product Characteristics

[32] https://www.fiware.org/

- It is a vendor-neutral open platform. Common API: FIWARE NGSI is being promoted, and it is active in more than 120 cities in 24 countries. Their data is operated and stored at distribution style and accumulation style. This system contributes to storing of unnecessary personal data.
  - FIWARE is an application of data utilisation in social and public fields. Initiatives by the public-private partnership between the EU and private companies for the purpose IoT platform that is a typical example of IoT Platform development project and its deliverables
  - FIWARE is a data management platform that focuses on cross-disciplinary data distribution. It is composed of about 40 types of module groups in 7 categories and can be freely combined and used according to the application. Each module is specified by "Next Generation Service Interface (NGSI)" standardized by OMA (Open Mobile Alliance), and data is passed through this.

- Distribution Channel
  - Web
- Security Characteristics
  - In cooperation with numerous standardisation bodies, FIWARE NGSI and Context Broker technology were announced as a component of CEF (Connecting Europe Facility) on February 5, 2018
- Business Model
  - Free
- Pricing
  - Free
- Strengths
  - A market-ready open source software, combining components that enable the connection to IoT with Context Information Management and Big Data services in the Cloud.
- Weaknesses
  - Many components exist and integrators have to choose them properly to meet the purposes.

On the following table, a summary of the conducted competitors' analysis can be found.

Competitor Name	Description	Target User	Distribution Channel	Business Model	Pricing	Strengths	Weaknesses
Secure IoT Platform	Promote security standardisation initiatives that include everything from the manufacturing stage of IoT devices to services in the cloud environment	Japanese ICT system vendors and device makers	Web and distribution with Hardware Partners	Membership	Not available	• IoT security standards that can be used for Japanese IoT market • Participation of some major security vendors	• Activities are based on research not actual business • Focused only in Japan
IoT Guardian Discovery	AI-powered, cloud-based platform that detects, identifies, secures, and provides insights into IoT devices.	Network managers and smart-city infrastructure management sectors	Partnering with global major ICT companies, such as Cisco and VMWare	License fee from using the platform + optional services based on demand.	Not available	• AI based security • Major partners • Security Operation Center support security management • Dashboard has good usability • Real time situational awareness	• Smart city is just one of its usage, therefore it has not unique smart-city-based characteristics
Kudelski IoT Security Platform	Industry-specific solutions secure the IoT use cases and applications that will transform your business. design trust & control into your IoT products and ecosystem from the start	IoT system and service providers	Unclarified	License fee from using the platform	Not available	• Partnership with major public cloud providers • Device management • Involvement in design phase of IoT devices • Support client's business model • Lifecycle support of IoT devices	• Smart city is just one of its usage, therefore it has not unique smart-city-based characteristics
Mainflux	Open-source IoT platform with the complete full-scale capabilities for development of Internet of Things solutions, IoT applications and smart connected products.	Municipality & Enterprise	Web and distribution with Hardware Partners	Open source	Free	• Built as a set of microservices containerized by Docker and orchestrated with Kubernetes, Mainflux IoT platform serves as a software infrastructure and middleware	• Insufficient way to earn money. They intend to do through consultation service
FreeRADIUS	FreeRADIUS project, the open	Used by huge	Major OSS	Open Source	Free	• Digital authentication • Long history of its safety	• Covering just small part of IoT security platform

	source implementation of RADIUS, an IETF protocol for AAA (Authorisation, Authentication, and Accounting).	amount OSS software developers. It is used for digital authentication	distributers, such as RedHat, are involved in its distribution			• 100 million users	and function.
Fiware	Open sustainable ecosystem around public, royalty-free and implementation-driven software platform standards that eases the development of new Smart Applications in multiple sectors	Municipality & Enterprise	Web	Open Source	Free	• A market-ready open source software, combining components that enable the connection to IoT with Context Information Management and Big Data services in the Cloud.	• Many components exist and integrators have to choose them properly to meet the purposes.

Table 2 Competitors' analysis summary

Competitor's analysis has been developed and some of strength and weakness on M-Sec positioning are clarified. M-Sec strength is security techniques and software such as the end-to-end point security, Blockchain and anonymization techniques. On the other hand, M-Sec does not have association with hardware Partners or vendors regarding distribution channel which could be considered as weaknesses. Moreover, sustainability and clear business model is still under development.

SME IoT Platforms are often offered at a lower price than large companies. Some companies offer their services as subscriptions for the usage of the platform.

SME products may have features not found in major companies by focusing on specific functions such as video analysis of live data, security techniques of data protection. However, not all service layers are developed like a big company Platform. In addition, the applications covered are very generic not providing a concrete use case for smart cities.

4. SWOT

A SWOT (strengths, weaknesses, opportunities and threats) analysis is provided below, updated from the previous version submitted on M12, in "D5.6 - Market Analysis and Exploitation". Competitors' analysis and technical progress and development of M-Sec have been taken into account on this new version of the SWOT in order to identify and analyse the internal and external factors that can have an impact on the viability of the M-Sec framework. Overall, the SWOT analysis provides a list of barriers (weaknesses and threats) and drivers (strengths and opportunities).

- Strength
  - Support for the implementation of two large smart cities such as Santander and Fujisawa
  - Scalability and Interoperability
  - Open source technology
  - Support for publish/subscribe and client-server type of protocols
  - Possibility of programming applications that would run on top of M-Sec with actuation possibilities
  - Participation of multiple partners with different expertise facilities for building a robust framework
  - Network monitoring
  - Endpoint event detection
  - Web transparency tools
  - Enterprise digital rights management
  - GANonymizer; featured anonymization system
  - Blockchain framework to facilitate the convergence of IoT security
  - Data collection and distribution with a unified way of accessing to underlying heterogeneous data sources
  - Rapid and simple development of end-user applications
  - Highly Innovative concept
  - Freemium approach where to experiment on top of it.
  - Smart City centred

- Weakness
  - Support, maintenance and operational costs. Framework sustainability once the project is finalised
  - Security of the involved systems which are being developed is not guaranteed
  - Lack of distribution with Hardware Partners or vendors
  - Immature TRL of the M-Sec core system components
  - No funding beyond the length of the project
  - Functionalities issues by integrating all the security layers

- Opportunity
  - Rapid growth of IoT devices. Estimated to increase to 41 Billion by 2025
  - Changes in data privacy law which will strengthen security adoption on the IoT ecoystem
  - Low competition offering the same type of concept. Most of the platforms do not include an end-to-end multi-layer security
  - Increase of attacks against IoT. During 2018, 32.7 million IoT attacks were detected33. Due to the high number of IoT attacks, solutions like M-Sec can be really well received in the market.
  - Awareness raised about the protection of personal information
  - Large wave of urbanisation. Cities need to unlock the value of data

- Threats
  - Increase of attacks against Internet of Things (IoT).Despite the security measures implemented by different solutions in the market, the volume of attacks is still very high
  - Impact of data is strongly connected to an effective data collection, management, processing and interpretation
  - Evolving security threats
  - Cyber attacks are related not only to data fraud and critical information infrastructure breakdowns, but also to profound social instability, interstate conflict, and failure of national governance
  - Overall unclear roadmap for innovative technology adoptions

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

5. Stakeholders' Analysis

It is crucial to ensure that the M-Sec project engages with the right stakeholders from its early stages, and that no effort is being wasted to communicate to the audiences that are less relevant to the project. For these reasons, during the second year of the M-Sec, the main aim has been to conduct a stakeholder mapping process in order to identify which stakeholders need to be engaged, to achieve the highest impact for the project.

Figure 7. Stakeholders' Engagement Process

5.1 Stakeholder Mapping Methodology

For the Stakeholders' Mapping, the Consortium has used the Power Interest Grid, which is also known as the Power Interest Matrix, a simple tool that helps to categorise project stakeholders with increasing power and interest in the project.

For that, a first step has been to identify the list of stakeholders that may be interested on such a project.

A second step has been to classify all the stakeholders into four categories based on their interests, benefits obtained and power of influence[34]:

- High power - High interest (Manage Closely): these stakeholders are decision makers and have the biggest impact on the project success and hence their expectations must closely managed.
- High power - Low Interest (Keep Satisfied): these are the stakeholders needed to be kept in loop and satisfied, even though they are not interested, because they yield power. This type of stakeholders should be dealt with cautiously as well, since they may use their power in a not desired way in the project if they become unsatisfied.
- Low power – High interest (Keep informed): people to keep adequately informed and talk to them to ensure that no major issues are arising. They can often be very helpful with the details of the project.
- Low power - Low interest (Monitor): These people should be monitored but not be bothered with excessive communication.

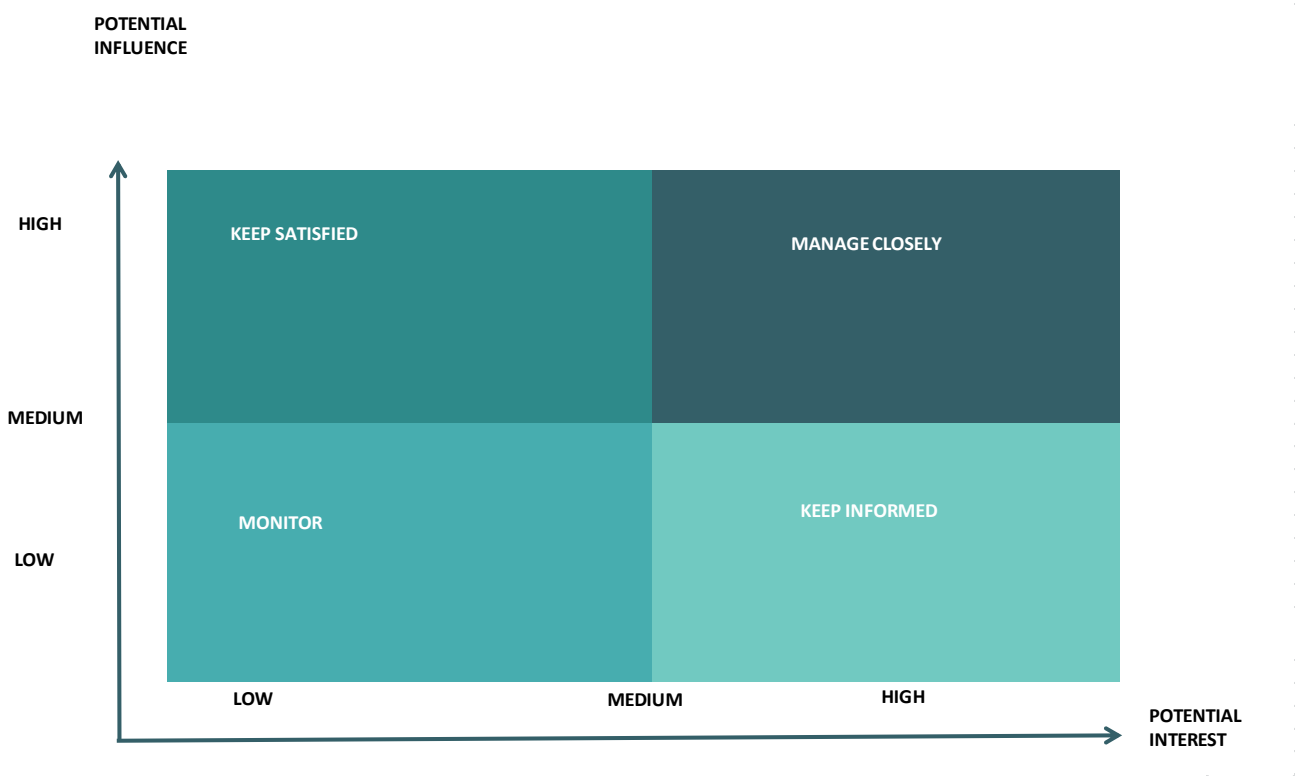

Figure 8. Sample Stakeholder's Position

The third step on the procedure, once stakeholders have been classified into these four categories, is to define the communication plan for finally engaging them. For this, "D5.9 - Community Building Plan" describes the actions to be taken in order to engage with Stakeholders. Finally, all the activities carried on by the Consortium to engage with Stakeholders during the second year as well as the plan for the last year of project can be found on in "D5.4 - Dissemination Activities".

[34] https://www.projectmanagement.com/wikis/368897/Stakeholder-Analysis--using-the-Power-Interest-Grid

5.2 Stakeholder Mapping Results

In this section, the consortium identifies the M-Sec stakeholder groups, the main challenges they face, the main benefits that they could obtain from M-Sec as well as the main areas where they could create impact and influence for future M-Sec adoption. Based on the analysis, stakeholders are mapped into different categories being the basis for future dissemination campaigns and focalisation of efforts for the exploitation.

- **Public Administration:** Municipalities, city council and city administration, National and Regional Governments
  - Challenge: The main challenge for public institutions is to find and deploy easily scalable technologies that bring tangible benefits (better services, reduced costs, meet citizen's needs), but that at the same time include reliable and robust security and privacy mechanisms to deal with any potential malicious attack o breach of sensitive information. The following points provide a summary of the main issues on deploying IoT Applications in terms of the project scope, Smart City IoT Security:
    - A cyberattack or data leak could have devastating consequences for a city and its citizens. For that reason, detecting malicious activity and blocking suspicious traffic, as well as enforcing other safeguards is a priority
    - Lack of accepted security standards or processes to follow
    - Regional, collaborative approach (bringing other municipalities into the conversation to share resources not only helps in lowering costs, but also ensures innovation does not stop at city borders)
    - Difficulty on meeting real citizen needs with Use Cases
    - Difficulty on quantifying social and economic benefits of IoT applications
  - What aspects of M-Sec are they likely to be interested in?
    - Smart City Use Cases Validation and evaluation Results (participants engagement, security KPIs, etc.)
    - Overall Project outcome results (such as deliverables of risks and threats analysis, APIs, Marketplace)
    - Open-Reference Architecture to include end-to-end security in their smart cities infrastructure
    - Access to relevant city data through the M-Sec Marketplace
  - Times or context in which they have more/less influence over the outcomes of M-Sec, ways they might block or facilitate the M-Sec impact
    - Promote the development and adoption of innovative Smart City Use Cases through M-Sec as a low-cost, flexible and open-reference architecture
    - One of the duties of government is to address market failures. Therefore, by creating regulations to penalize businesses that do not take security seriously enough, government can positively influence on the use of M-Sec
    - Deploy IoT Smart City Application of top of M-Sec Components
  - Key Message
    - M-Sec looks forward to working closely with Government and Smart Cities to enforce Data protection whilst continuing to promote innovation within the IoT Ecosystem

- **Developers:** Independent programmers who are willing to experiment & engage with M-Sec components to build IoT applications on top.
  - Challenge:
    - Lack of security knowledge base of IoT developers. Fundamental security elements on the smart device side, including secure boot, thing authentication, message encryption and integrity, and a trusted key management and storage scheme, are not always implemented. It is very challenging to define secure software/hardware development lifecycle guidelines for IoT, due to the many different hardware, protocols and network connectivity methods used in the IoT development.
    - Lack of expertise on applying security standards correctly along with the adoption of new regulations impact (i.e. GDPR)
    - Frameworks, tools, and libraries become outdated pretty quickly
    - Dealing with 3rd Party APIs
  - What aspects of M-Sec are they likely to be interested in?
    - M-Sec enables focusing on what is specific to add security on the smart IoT applications, making development much faster and compliance with regulations possible
    - The modular nature of M-Sec means that it is possible to re-architect as the need changes
    - Freemium version where to experiment with M-Sec secure components.
    - Through our Strong Community, it is possible to share experience with other developers
    - Access to APIs and Manuals for integrations
    - Access to the M-Sec Marketplace to exchange data generated by IoT Applications developed
  - Times or context in which they have more/less influence over the outcomes of M-Sec, ways they might block or facilitate the M-Sec impact
    - Provide technical support for the sustainability of the framework with own skills and get access to unlimited versions of the SW in return
    - Promote the adoption of M-Sec around the developer community
    - Deploy IoT Smart City Application of top of M-Sec Components
  - Key Message

    M-Sec eases the development of IoT Applications while reducing development costs and ensuring security with no need of expert knowledge to be compliant with the latest regulations through its secure framework based on end-to-end IoT Layer solution.

- **Research Centres & Universities:** Technical Universities and Research organisations boosting innovation projects with a practical application.
  - Challenge:
    - Understand the practical applicability of the research results i.e. Connectivity challenges (transport of data from the sensors and transmission of instruction to the actuators), Cloud based architecture (network delays, throughput, reliability), Security mechanisms, etc.
    - Visibility of the main achievements/created solutions.
  - What aspects of M-Sec are they likely to be interested in?
    - M-Sec Community to address and share challenges

- Strengthen cooperation with industry. Networking (sharing scientific expertise, potential collaboration). Possibility to participate (or even speak) at M-Sec events and establishing contacts with industry and other stakeholders
- Market insights
- Provision of access to relevant research Results on open issues about IoT in terms of security, APIs, etc.
- Fostering Research

- Times or context in which they have more/less influence over the outcomes of M-Sec, ways they might block or facilitate the M-Sec impact
  - M-Sec knowledge transfer for alumni and students
  - Sharing new findings on IoT security with partners from M-Sec
  - Disseminating M-Sec results on events, webinars, workshops
  - Engaging partners from M-Sec consortium into new research and innovation projects with the same subject of M-Sec where there is the possibility to reuse M-Sec outcomes
- Key Message
  - Be update with new findings to be at the forefront of research by becoming an active member of the M-Sec community

- **Policy Makers & EU Regulations:** Those responsible for formulating or amending IoT policies and standards.
  - Challenge:
    - Lack of information regarding barriers, challenges, findings found on new regulations adopted. For example, the main obstacles found on the new EU-JP adequacy agreement of data flow.
    - Lack of information to set proper IoT security Standards.
    - Lack of understanding of the IoT ecosystem: its main actors, value and benefits of the technology, needs of the key stakeholders, challenges they are facing, etc.
    - Difficulty on facilitating, co-developing and executing IoT security
  - What aspects of M-Sec are they likely to be interested in?
    - Access to the international network of IoT experts and other stakeholders
    - Opportunity to stimulate policy innovation regarding M-Sec findings
    - Awareness and insights on effective Data Protection regulation and implementation through our two cross border use cases
    - Practical and proven M-Sec solution to develop Data Protection standards on the IoT Ecosystem
  - Times or context in which they have more/less influence over the outcomes of M-Sec, ways they might block or facilitate the M-Sec impact
    - Gather information related to M-Sec research, challenges, findings and implementations to extract from this information, a policy or a set of policies which serve to promote and strengthen security in IoT applications
  - Key Message
    - M-Sec will validate through its two crossborder use cases the new Adequacy Agreement between EU&JP that allows the transfer of personal data without additional safeguards between the EU and Japan

- **Citizens:**
  - Challenge:
    - Lack of confidence or reluctance to IoT ecosystem
    - Issues regarding protection of personal data.
    - Not feeling attracted with available Smart City Use Cases.
    - Lack of transparency of the smart city governance
  - What aspects of M-Sec are they likely to be interested in?
    - Participation on the M-Sec Pilots Implementations to validate the secure solution.
    - How M-Sec can provide additional security on personal data processed.
  - Times or context in which they have more/less influence over the outcomes of M-Sec, ways they might block or facilitate the M-Sec impact
    - Participate on pilot tests to validate the developments and innovation within M-Sec.
    - Be less reluctant to adopt IoT innovative Smart City Applications
  - Key Message
    - M-Sec will bring new IoT security standards to ensure end-to-end data privacy by building a reliable and trustworthiness IoT ecosystem.

- **IoT Providers:** IoT devices and sensors, services and applications providers, integrators.
  - Challenge:
    - Hardware Manufacturers:
      - Outdated Hardware. Difficulty to keep devices with enough updates as manufacturers are focused on building new ones to continuously bring value added to the marked and keep competitive position.
    - Hardware Manufacturers, application providers and integrators
      - Competitive pressures for shorter times to market and cheaper products drive many designers and manufacturers of IoT systems (including devices, services and applications), to devote less time and resources to security.
      - Low-cost, low-complexity model of most IoT devices means IoT providers have little incentive to add security functions beyond GDPR compliance.
  - What aspects of M-Sec are they likely to be interested in?
    - M-Sec enables to focus on what is specific to add security, making development much faster and compliance with regulations.
    - Reduced development costs while providing solutions beyond GDPR compliance.
    - The modular nature of M-Sec means that is possible to re-architect as the need changes.
    - Sandbox environment where to experiments with M-Sec secure components.
    - Through our Strong Community, it is possible to share experience with other stakeholders.
    - Access to APIs and Manuals for integrations
  - Times or context in which they have more/less influence over the outcomes of M-Sec, ways they might block or facilitate the M-Sec impact
    - Adoption and use of M-Sec framework.
    - Dissemination among other industries companies about the benefits obtained through M-Sec

- Key Message
  - "M-Sec will bring new IoT security standards to ensure end-to-end data privacy by building a reliable and trustworthiness IoT ecosystem.

- **Telecom Operators:**
  - Challenge:
    - By 2021, Gartner estimates that some 25 billion IoT devices will be connected to telecom networks. Preventing unauthorized access, securing data transmissions and ensuring smooth monitoring of a much larger attack surface are the key security challenges for telcos35.
    - Operators have a strong legacy in securing the connectivity layer with carrier-grade, embedded security solutions. Security requirements such as secure transmission, safe data and user authentication have been fused into the operator networks for decades and cellular networks are generally viewed as secure and reliable. However, moving up the value chain requires more specialist security expertise[36]
  - What aspects of M-Sec are they likely to be interested in?
    - Having good IoT security into the networking equipment can present revenue opportunities for mobile telco operators as they seek to expand from the commoditized services of basic connectivity to more value-add services. Therefore, they may be interested on the secure components developed within the frame of M-Sec
    - Since Telecom Operators do not count with security expertise in the whole IoT chain, they may be interested on making partnership to share security expertise.
  - Times or context in which they have more/less influence over the outcomes of M-Sec, ways they might block or facilitate the M-Sec impact
    - Adoption and use of M-Sec framework.
    - Potential Partnerships with M-Sec partners.
  - Key Message
    - "M-Sec is composed by several partners with expertise in different technologies (IoT, blockchain, cloud). Therefore, security expertise is provided along with a set of secure components to guarantee and ensure end-to-end security at the whole IoT chain".

[35] https://www.infopulse.com/blog/security-telecom-threats-and-solutions/
[36] https://www.analysysmason.com/research/content/comments/operators-iot-security-rdme0/

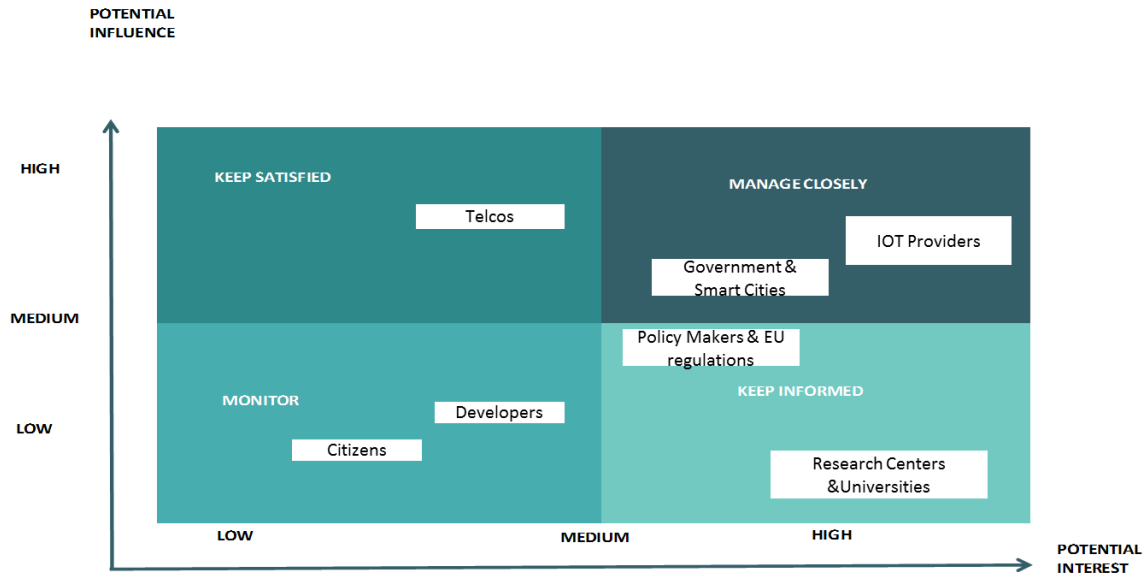

Figure 9. M-Sec Stakeholder's Position

As a summary, we provide below a figure indicating the value proposition per stakeholder that has resulted from the analysis and that is taken into account on section 6 M-Sec Business Model Canvas and Value Proposition

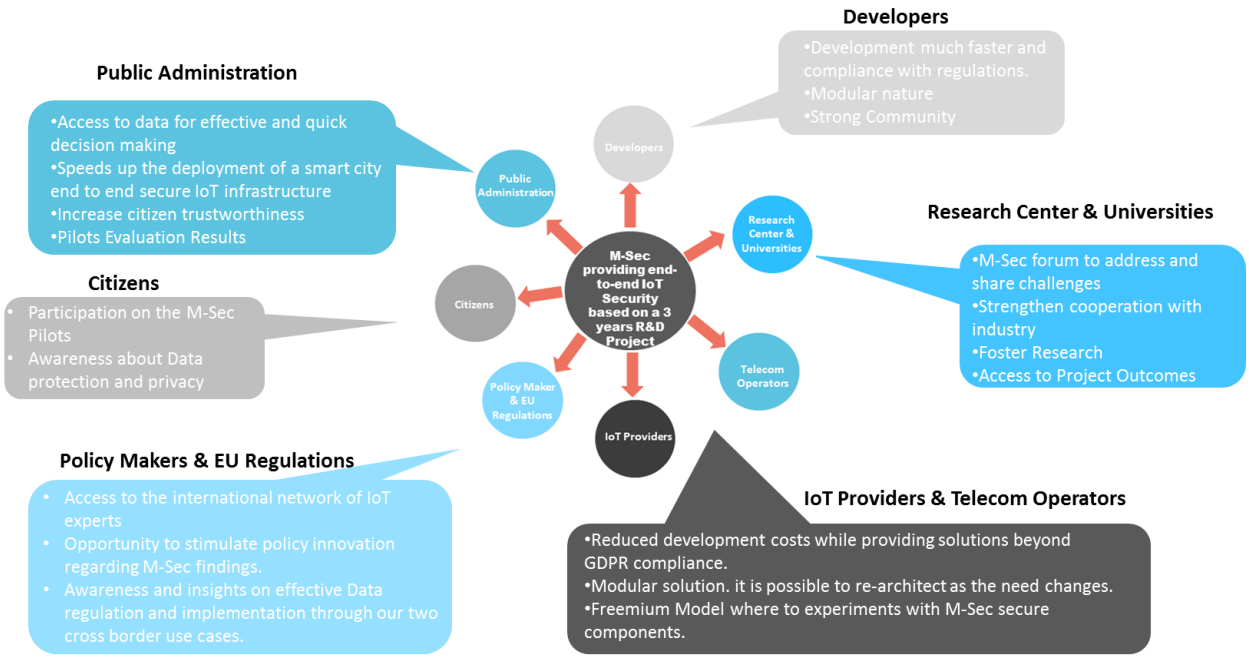

Figure 10. M-Sec Stakeholder's Value Proposition

6. M-Sec Business Model & Value Proposition

6.1 What is M-Sec?

M-Sec's aim is to provide a low-cost and flexible end-to-end secure IoT Framework extending security mechanisms from the device to the cloud and to the application, in a seamless and fully integrated manner.

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

In the figure below, the end-to-end security value added by M-Sec through the different layers is shown.

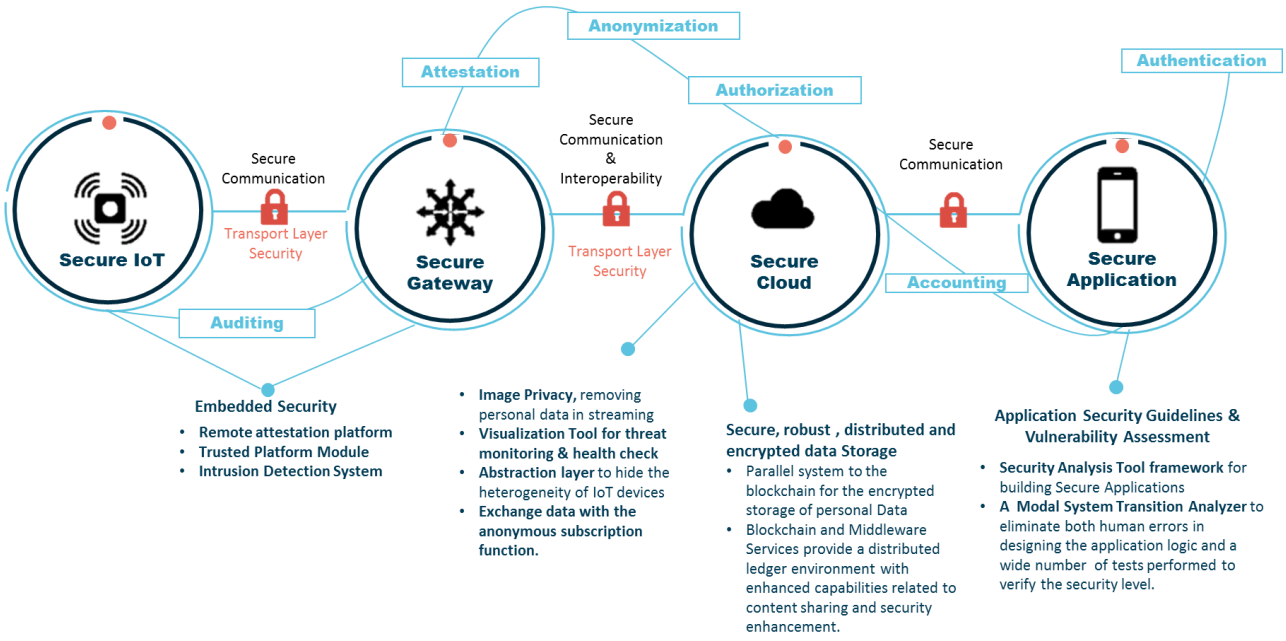

Figure 11. M-Sec End-to-end IoT Security Application

M-Sec, additionally to its secure end-to-end framework, enacts a Marketplace for third parties to develop secure applications and services around secure application/cloud/IoT elements. The Marketplace framework allows secure IoT data exchange between data providers and consumers. In order to boost replicability of the different M-Sec Use Cases that will validate the M-Sec framework, the consortium has considered to make the Marketplace central to all use cases, allowing to publish anonymised data coming from the different sensors e.g. from environmental sensors to home IoT devices.

Through the M-Sec Marketplace, market participants (from IoT devices to humans using mobile applications) are able to exchange data and value through the M-Sec blockchain implementation and Smart Contracts specifically created under the context of M-Sec.

The M-Sec Marketplace:

- can provide various tokens and transactions models, based on the specific requirements of each applications domain
- provides the environment for the seamless creation of smart-contracts based on the corresponding business-models behind specific markets and applications.

The final goal for a city to become smart is having access to information and using 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.

On the following figure, the consortium defines the main benefits obtained through M-Sec Project.

Figure 12. M-Sec Benefits

6.2 The M-Sec Mission and Vision

M-Sec's mission is to provide market-ready open-source software, combining multiple secure components to enhance security on multiple IoT layers (device, cloud, and application), facilitating and accelerating Smart city applications' development and ensuring trustworthiness in ecosystems between different actors and addressing security and privacy issues in all layers to ensure "end-to-end security and privacy".

M-Sec's vision is to boost awareness and adoption of IoT Security Mechanisms for further deployments of M-Sec results in other IoT infrastructures and smart cities throughout Europe and Japan

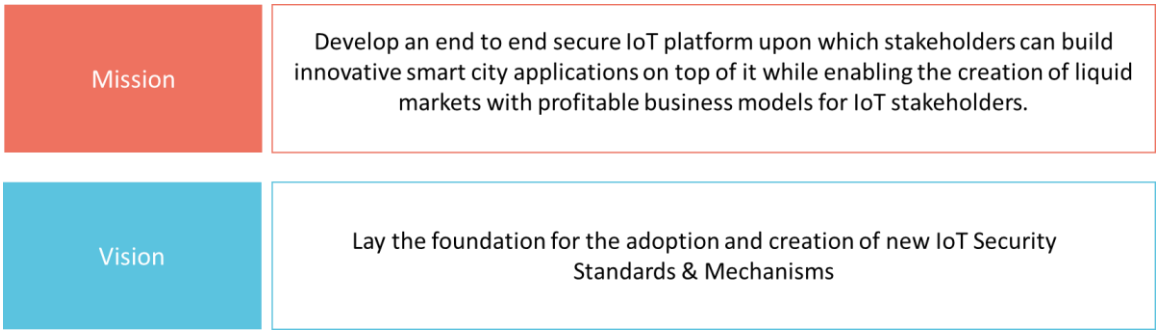

Figure 13. M-Sec Mission and Vision

6.3 M-Sec Business Model Canvas & Value Proposition

In this subsection, we describe the building blocks of the M-Sec Value Proposition and Business Model. There are many ways of describing a value proposition and business model. However, the consortium has followed the Canvas guidelines developed by Dr. Alexander Osterwalder.

The Value Proposition Canvas is formed around two building blocks – customer profile and a company's value proposition[37]:

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

[37] https://www.b2binternational.com/research/methods/faq/what-is-the-value-proposition-canvas/

In the following figure, the consortium provides the value proposition of M-Sec as a whole, including the Secure IoT framework and the Marketplace.

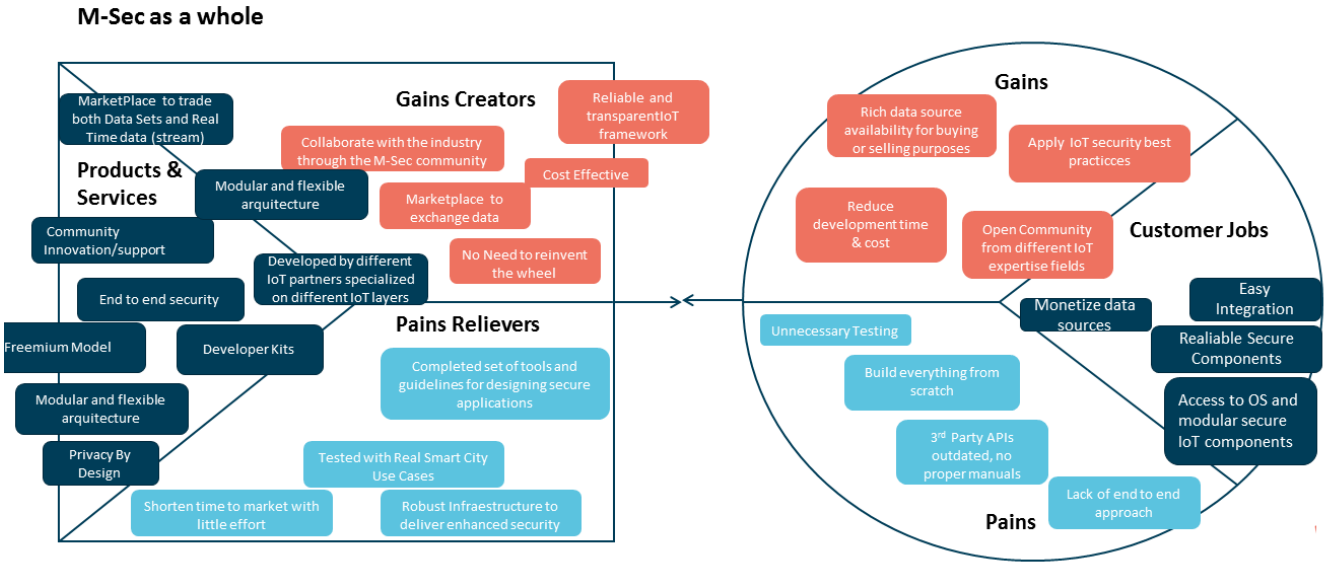

Figure 14. M-Sec as a whole Value Proposition

Once the value proposition has been set, the next step is to conduct the Business Model Canvas of M-Sec with nine different building blocks explained below[38].

The building blocks of the Business Model canvas consist of the following topics:

1. Customer segment
2. Value proposition
3. Channels
4. Customer relationship
5. Key activities
6. Key Resources
7. Key partners
8. Revenue stream
9. Cost structure

- 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?

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

- 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

Each of the building blocks is further described in separate chapters below.

6.3.1 Customer Segment

For customer segment, stakeholders have been already identified on section 3 Stakeholder's Analysis.

- Government & Smart Cities
  - Municipalities
  - City Council
  - National and Regional Governments
- IoT Providers (IoT manufacturers, cloud service providers, applications providers, integrators)
  - Startup & SMEs
  - ICT Companies
- Policy makers & EU regulations
- Research Centers & Universities
- Developers
- Citizens
- Telecom Operators

6.3.2 Value Proposition

Table 3. Value Proposition

#	Problem	Solution Offered by M-Sec
VP1,7	Lack of a Communities focused on Security IoT challenges and developments to share findings and boost innovation	A community with expert partners on several technologies where links among incubators, business networks, universities and developers communities are provided to share IoT challenges and findings.
VP2,3&9	Competitive pressures for shorter times to market and cheaper products drive many designers and manufacturers of IoT systems (including devices, services and applications), to devote less time and resources to security.	A market-ready open source software, flexible, modular and decentralized architecture to build experiments. Easy integration, including Developer Kits and APIs Documentation.
VP4	Lack of knowledge regarding security aspects for secure software development.	M-Sec provides Application Security Guidelines &

			Vulnerability Assessment.
	VP5	There are increasing numbers of smart city platforms being proposed by different vendors. However those solutions are often locked-in by design and cannot share data with one another, which causes market fragmentation and poor user experience.	A secure and modular framework to plug&play connection support to a large number and type of existing platforms and protocols while at the same time provides a fine grained security mechanism to allow access to services by only authenticated and authorised entites.
	VP5	The rise in the adoption of IoT has increased the potential of cyberattacks. Cybercriminals seek to exploit susceptibilities in smart devices manufactured with poor security practices.	M-Sec provided an End-to-End Secure IoT Modular Framework based on solutions covering multiple IoT layers (device, cloud, application). With intrusion detection mechanisms, removing sensitive data in stream, encrypted data storage tamper proof, lightweight cryptosystem, seamless hyper-connectivity, threat monitoring vulnerability assessment.
	VP5	In situations where video data is used impose new threats to privacy	A tool that automatically deletes personal information contained in such videos using AI technology.
	VP5	Ensuring that information remains secure, private and authentic has become an ongoing challenge. Using blockchain technology, some of the issues can be addressed. However, once data is stored on the blockchain it can't be manipulated or altered.	A parallel system to the blockchain for the encrypted storage where sensitive data is encrypted together with a hash. Thanks to the M-Sec Blockchain and Middleware it is possible the synergy

			between on-chain and off-chain data and access control, through enhanced Transactions and Meta-data handling, providing anonymity through the Know Your Customer service and enabling the extension of the system with higher-level services such as Trust & Reputation Management, Proof of Location mechanisms, etc.
	VP5	Due to explosive growth of Internet of Things (IoT), billions of IoT devices have surfaced in all aspects of life. This has provided a harvesting ground for bad actors to attack and compromise IoT devices to be used as Botnets for further attacks.	M-Sec provides Intrusion Detection mechanisms & Visualization tool to monitor malicious activity or policy violations. Additionally, the consortium has developed a Secure element to handle the integrity of the device during the boot process and the authentication and encryption for external communication channels. With these elements, M-Sec ensures the prevention of malicious attacks, the Integrity of IoT devices and the Availability of IoT devices.
	VP5	The nature of IoT with its heterogeneous architecture and devices involve the sharing of information and collaboration between things across many networks. This poses serious challenges to the end-to-end security.	A directory service containing all information to manage security services for clients, such services known as AAA for Authentication, Accounting and Authorization.
	VP6	Barriers for accessing data and transform	M-Sec provides a secure Iot

	data sources from a discrete use to a multi-use paradigm. Data accessibility and interoperability along with privacy and security concerns.	Marketplace to exchange data and put in contact data providers with data consumers.
VP8	Innovative solutions sometimes are not mature enough. Difficulty on meeting real citizen needs with interesting IoT Applications and to evaluate and quantify social and economic benefits of IoT applications.	Practical and Proven solution. M-Sec Framework will be validated through the implementation of 5 different Use Cases ranging from environmental IoT devices to home monitoring sensors.

6.3.3 Channels

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

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

6.3.4 Customer relationship

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

6.3.5 Key Activities

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

6.3.6 Key Resources

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

- European Funding Programmes
- High Technical Skilled Human Resources

6.3.7 Key Partners

- Pilot Cities
- M-Sec partners
- European Commission
- Smart Cities Strategic Alliance
- Relevance Standardisation Bodies
- Strategic Partnerships per Domain
- Data Providers

6.3.8 Cost Structure

- Product development and maintenance cost
- Personnel Cost
- Marketing Cost
- Infrastructure Costs

6.3.9 Revenue Stream

- Marketplace Monetization / Subscription
- Freemium Model
- Advertising
- Consultancy Services
- Integration Support
- Project Funding
- Licensing

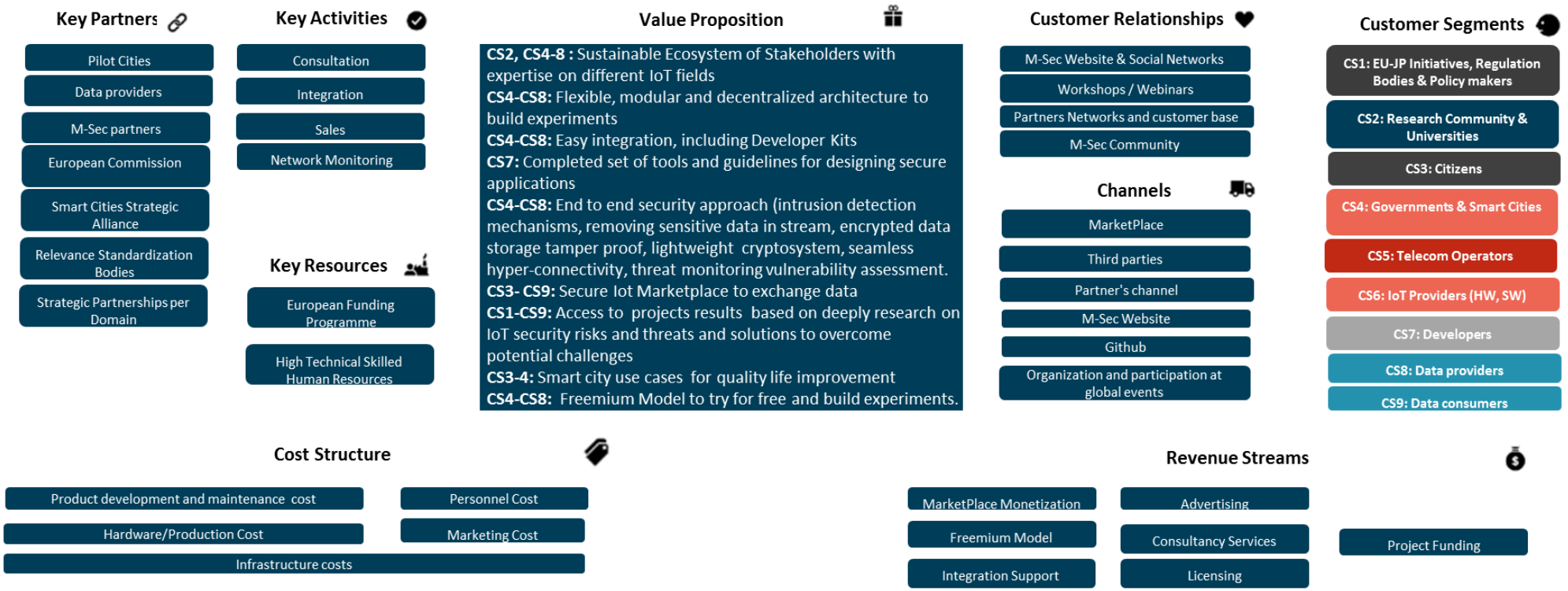

Figure 15. M-Sec Business Model Canvas

7. M-Sec Components and IPR Management

In order to avoid potential issues that may arise in the future commercialization activities which could have a negative impact on the project's outcomes, the consortium has identified the software components developed and enhanced within the project, specifically within WP4 "Multi-Layered Security Technologies". For each software component, the applicable license for exploitation purposes based on the minimum possible license on the libraries used in each case has been identified. Further details such as ownership, technology used, whether the software component can be individually exploitable and if it they are part of the core or an extension module can be found on the following subsections.

7.1 M-Sec Components IPR & Licensing

As mentioned previously, the consortium has generated a table that provides the following information:

- The M-Sec functional group component, which represents a reusable, functional, identifiable part of the whole framework that provides a set of functionalities based on the combination of other components.
- A sub-component represents a smaller functional part that in a combination with other sub-components, introduce the functional group component.
- The ownership column is related to M-Sec partner's right to use, manage, the right to possess a certain component. At this stage, we might also refer to the ownership as partner responsible for the development of such component, or the legal ownership in case the component was developed before the M-Sec project.
- Technologies used column is covering the programming languages and databases used for the development of the (sub-) component.
- Software libraries and frameworks are standard or custom libraries created by partners for a given component.
- Can be the component exploited individually? This column indicates if the component can be used independently. That is, if the component can be sold without any dependency on other component.

7.2 Types of Software Licenses

The major type of software licenses can be classified as following:

1. Proprietary
2. Free and Open Source
3. Copyleft
4. Dual Licensing
5. Multi Licensing

There are a number of considerations that have to be made by each partner when choosing the appropriate license for the components developed at WP4. For example, components that may be potential to patent,

whether future software can be used commercially, allows the redistribution and modification, allowed for private use, require the disclosure of the source code or license and copyright notice, state changes and liabilities, etc.

7.2.1 Types of Open Software Licenses

The following OSI-approved licenses are popular, widely used, or have strong communities[39]:

- Apache License 2.0
- BSD 3-Clause "New" or "Revised" license
- BSD 2-Clause "Simplified" or "FreeBSD" license
- GNU General Public License (GPL)
- GNU Library or "Lesser" General Public License (LGPL)
- MIT license
- Mozilla Public License 2.0

Most relevant open source licensing standards							
	Linking	**Distribution**	**Modification**	**Patent grant**	**Private use**	**Sublicensing**	**TM grant**
Apache License 2.0 (Apache-2.0)	Permissive	Permissive	Permissive	Yes	Yes	Permissive	No
3-clause BSD license (BSD-3-Clause)	Permissive	Permissive	Permissive	Manually	Yes	Permissive	Manually
2-clause BSD license (BSD-2-Clause)	Permissive	Permissive	Permissive	Manually	Yes	Permissive	Manually
GNU General Public License (GPL)	GPLv3 compatible only	Copylefted	Copylefted	Yes	Yes	Copylefted	Yes
GNU Lesser General Public License (LGPL)	With restrictions	Copylefted	Copylefted	Yes	Yes	Copylefted	Yes
MIT license (MIT)	Permissive	Permissive	Permissive	Manually	Yes	Permissive	Manually
Mozilla Public License 2.0 (MPL-2.0)	Permissive	Copylefted	Copylefted	Yes	Yes	Copylefted	No

Figure 16. Most relevant open source licensing standards

7.2.2 M-Sec Licenses requirements

For successful future exploitation, the following requirements must be considered:

- Possibly open source license-type that should also be open in terms of interfacing (e.g. public APIs)
- Exploitation wise there should be a possibility to combine M-Sec results/software and components with third party software or libraries. Ideally it should not contaminate third party software with M-Sec own OS license
- and finally, it of crucial importance is to be able to change the license type at later stages and when the framework is ready for commercialization if required by the post-M-Sec business model.

[39] https://opensource.org/licenses

In order to facilitate understanding of the different components to be evaluated for IPR, below it is included the architectural view that can it can be also found in D3.4 “M-Sec Architecture – functional and technical specifications final version”.

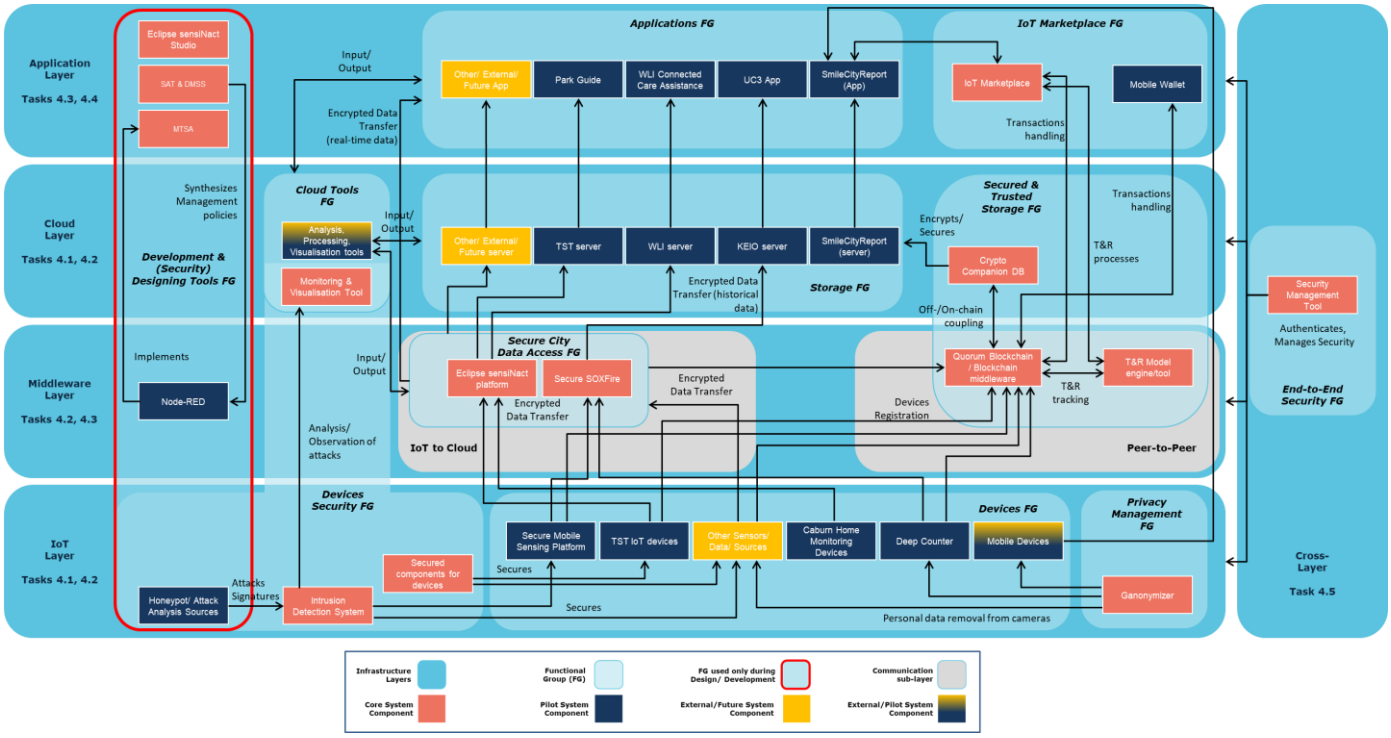

Figure 17. M-Sec Architecture View

On the following table, both the M-Sec core system components and the pilot system components are listed and categorised by functional group and corresponding IoT Layer. For better understanding, a description of the secure functionality is provided by each component.

Table 4 Overview of M-Sec Core System Components

Functional Group	Layer	Component	Description
Development & Security Designing Tools	Application	Security Analysis Tool & Development Method for a secure service (SAT & DMSS)	A security requirements modelling support system, for a misuse case diagram that enables the association of security knowledge with elements that constitute the diagram.
	Application	Modal Transition System Analyser (MTSA)	A development tool for synthesizing behaviour specification for reactive systems with formal guarantee.
	Middleware	Node-RED	Node-RED is a flow-based development tool for visual programming developed originally by IBM for wiring together hardware devices, APIs and online services as part of the IoT.
	IoT	Honeypot (IoTPOT)	Tool to obtain knowledge on the attack vectors of IoT devices (such as IP cameras, network drives, Wi-Fi, sensors, etc.) through observation and analysis of various types of attacks from internet.
Secured & Trusted Storage	Cloud	Crypto Companion Database (CCDB)	As the real world matches the digital world, ensuring that information remains secure, private and authentic has become an ongoing challenge. Using blockchain technology, some of the issues can be addressed. However, once data is stored on the blockchain it can't be manipulated or altered. Our companion database is proposed as a parallel system to the blockchain for the encrypted storage. The blockchain saves a hash created from sensitive or personal data, and the companion database stores the sensitive data encrypted together with the hash.
	Middleware	Quorum Blockchain	A distributed ledger and middleware services system which provides all the necessary groundwork

		& Blockchain Middleware	for security/privacy-enhancing services related to transactions and interactions between actors of various ecosystems.
	Middleware	Trust & Reputation Model/Engine	The Trust & Reputation Management Engine (T&RM Engine) is a tool working on top of the M-Sec blockchain/Marketplace and in parallel with the corresponding middleware so as to provide a ranking system assessing the reliability, trustworthiness and reputation of resources providers within the M-Sec ecosystem.
IoT Data Marketplace	Application	IoT Marketplace	The M-Sec IoT Marketplace is a novel Marketplace where smart objects and users can exchange information and services through the use of virtual currencies, allowing real-time matching of supply and demand, and thus enabling the creation of liquid markets with profitable business models of the IoT stakeholders.
	Application	Mobile Wallet	Mobile Wallet enables users to manage directly their transactions and get access to the content within the Blockchain.
Secure City Data Access	Middleware	Eclipse sensiNact platform and Studio	SensiNact is designed to allow platforms to interoperate, thus coexist and benefit from the richness of the variety. Additionally, it provides a fine grained security mechanism to allow access to services by only authenticated and authorized entities.
	Middleware	Secure SOXFire	SOXFire can provide practical distributed and federated infrastructure for IoT sensor data sharing among various users/organisations in a way that is scalable, extensible, easy to use and secure, while preserving privacy.
Devices Security	IoT	Secured components for devices and gateways	A secure element, such as a TPM, is added to the physical platform, It is used to store any sensitive information that shall be protected from people having physical Access to the electronics, such as IoT devices and gateways. The secure element handles the integrity of the device during the boot process and also handles the authentication and encryption for external communication channels.
	IoT	Intrusion Detection	Protect vulnerable IoT devices from malicious activities using defense-in-depth mechanisms and

		System (IDS)	threat monitoring, thereby providing multi-layered security against policy violations and cyber attacks, along with security health-checks
	IoT	Monitoring & Visualisation tool	A software-based solution that collects and examines activity from IoT layer or agents embedded in the IoT gateway devices. This tool not only help with the security health checks by providing insight into how the security is being maintained at IoT gateways, but also helps in further analysis of devices under attack. Thereby, providing 24/7 security threat monitoring and alerts.
End-to-end Security	Cross Layer	Security Management Tool	A set of centralized security functions that are necessary to ensure end-to-end security, privacy and therefore digital trust. It is designed to support several security functionalities aggregated in a single backend using the LDAP standard. The central element for the security manager is a directory service containing all information to manage security services for clients, such services known as AAA for Authentication, Accounting and Authorization.
Privacy Management	IoT	Ganonymizer	In situations where video data is used in various IoT application use cases such as smart cities, personal information is often a problem. GANonymizer is a technology that automatically deletes personal information contained in such videos using AI technology.

Additionally to the M-Sec Core System Components, on the table below we include the Pilots System components employed for the validation of the M-Sec technology developments.

Table 5 M-Sec Pilot System Components

Component	Layer	Description
Park Guide	Application (UC1)	The Park Guide application offers end users a channel to interact with the IoT devices deployed in Use Case 1 in Santander. Upon their registration in the system end users will get access to the real time measurements offered by the IoT devices and will take part of an M-Sec community

		where they will take part of joint games.
Worldline Connected Care Assistance	Application (UC2)	Dashboard for Tele-assistance operators to be able to monitor elderly homes with the aim to improve the quality of life of elderly people living alone and conduct decision-making based on rules and alerts configured upon the activity collected by different home sensors.
Smile City Report	Application (UC4)	Smile City Report is a participatory sensing smartphone app that allows participants to record and distribute both out-camera photos and in-camera photographers photos on a common theme.
Deep Counter	IoT (UC3)	The Deep Counter automatically counts the amount of garbage from camera images attached to the garbage truck using Deep Learning. Deep Counter makes it possible to specifically quantify and analyse where and how much garbage is discharged.
Secure Mobile Sensing Platform	IoT (UC3)	The Mobile Sensing Platform is an open smart city platform that can share data between multiple cities, targeting not only physical IoT sensors but also data from smartphones as participatory sensing and data on the web.
TST IoT Environmental devices	IoT (UC1)	The IoT device retorts to a wireless communication technology (namely Sigfox or NB-IoT) to send periodically sensor measurements via MQTT and put them on a user interface that end users can check through a web or mobile application.
TST IoT crowd-counting devices	IoT (UC1)	The IoT device retorts to a wireless communication technology (namely Sigfox or NB-IoT) to send periodically sensor measurements via MQTT and put them on a user interface that end users can check through a web or mobile application and then take a peek to the spots most visited and well-received by their peers.
Caburn Home Monitoring Devices	IoT (UC2)	Home activity sensors (smart plug, motion sensor, bed occupancy sensor, door/window open sensor) and Gateway

For each of the components identified above, the consortium has included details regarding:

- Origin
  - Non M-Sec: Component brought by a partner before the initiation of the M-Sec project. No enhancements have been done
  - M-Sec developed: Component created within the project time frame
  - M-Sec extended: Component brought by a partner which has been further enhanced with security mechanisms
- Technology used covering the programming languages and databases used for the developments or enhancements and the SW libraries used
- Whether the component can be used independently without having to rely in any other component under a specific functional group,

Table 6. M-Sec Core System Components Licenses used for development

Functional Group	Component	Ownership	Origin	Technology Used	SW libraries used	Can be exploited?
Development & Security Designing Tools	Security Analysis Tool & Development Method for a secure service (SAT & DMSS)	NII	Non M-Sec	Java	Docker: Apache License 2.0 MySQL: GPL	Under investigation (3rd Year task)
	Modal Transition System Analyser (MTSA)	WU	Non M-Sec	Java	Docker: Apache License 2.0 MySQL: GPL	Under investigation (3rd Year task)
	Node-RED	WLI	Non M-Sec	JavaScript	Node.js: MIT	No
	Honeypot (IoTPOT)	YNU	Non M-Sec	Non-disclosure (Proprietary)	Non-disclosure (Proprietary)	No

Secured & Trusted Storage	Crypto Companion Database (CCDB)	WLI	M-Sec developed	MongoDB	Docker: Apache License 2.0 Oracle VirtualBox: GNU Git NPM: Artistic License 2.0 Mongo DB Server Side: Public License	Yes
	Quorum Blockchain & Blockchain Middleware	ICCS	M-Sec extended	Solidity Node.js Javascript IPFS jQuery HTML CSS Bootstrap	Solidity: GNU-GPLv3.0 Node.js: MIT IPFS: MIT, Apache 2.0 jQuery: MIT Bootstrap: MIT, Apache 2.0	Yes
	Trust & Reputation Model/Engine	ICCS	M-Sec developed	Soliditiy Javascript Node.js HTML, CSS, Bootstrap	Node-Red: Apache 2.0 Node.js: MIT jQuery: MIT Bootstrap MIT, Apache 2.0 Vue.js : MIT MariaDB: GPLv2, LGPLv2.1 Solidity: GNU-GPLv3.0 Python-Flask BSD	Yes
IoT Data Marketplace	IoT Marketplace	ICCS	M-Sec developed	Node-Red Node.js Javascript jQuery HTML CSS Bootstrap Vue.js MySQL Solidity	Node-Red: Apache 2.0 Node.js: MIT jQuery: MIT Bootstrap MIT, Apache 2.0 Vue.js : MIT MariaDB: GPLv2, LGPLv2.1 Solidity: GNU-GPLv3.0 Python-Flask BSD	Yes
	Mobile Wallet	WLI	Non M-Sec	Java, Javascript, Objective C	Angular: MIT license Cordova: Apache 2.0 License	Yes
Secure City Data Access	Eclipse sensiNact platform and Studio	CEA	M-Sec extended	Java/OSGi	https://projects.eclipse.org/proposals/eclipse-sensinact	Yes
	Secure SOXFire	KEIO	M-Sec	Openfire, Java,	Openfire 4.2.3 Apache2.0 JSoxlibv1.6 (None)	Yes

			extended	MySQL	Smack 4.2.2 Apache 2.0	
Devices Security	Secured components for devices and gateways	CEA	M-Sec extended	C	Das U-Boot: GPLv2+ Linux: GPLv2 TPM2-TSS: BSD 2 TPM2-TSS-Engine: BSD3 WolfSSL: GPLv2	Under investigation (3rd Year task)
	Intrusion Detection System (IDS)	YNU	M-Sec extended	C, C++, Python	OISF: GPL	No
	Monitoring & Visualisation tool	YNU	M-Sec extended	Elastic	Elastic Search: Apache2	No
End to end Security	Security Management Tool	CEA	M-Sec developed	C, Python, Java	Keycloak: Apache license 2.0 FreeIPA: GNUv3 OpenLDAP: OpenLDAP Public License v3 OpenSSL: Apache License 2.0 WolfSSL: GPLv2	Under investigation (3rd Year task)
Privacy Management	Ganonymizer	KEIO	Non M-Sec	Python	Pytorch: BSD Torchvision: BSD Numpy: BSD Scipy: BSD Scikit-image: BSD Opencv-python: BSD Pillow: MIT Matplotlib: BSD Pyyaml: MIT	No

Table 7. M-Sec Pilot System Components Licenses used for development

Component	Ownership	Origin	Technology used	SW libraries used	Can be exploited?
Park Guide	TST	M-Sec developed	MQTT, GPRS, Java, PHP SQL	jQuery 3, DataTables, bootstrap v1.2.3, Modernizr.js, Python's standard library 3.4.0, Paho MQTT Python	Yes
Worldline Connected Care Assistance	WLI	Non M-Sec	Nest, Node JS, Angular	MongoDB	Yes
Smile City Report	KEIO	M-Sec extended	Google Flutter, Framework, Dart, Ruby, Ruby on Rails, MySQL, Google Firebase	Runy on Rails: MIT MySQL: GPL	Yes
Secure Mobile Sensing Platform	KEIO	M-Sec extended	XMPP	Openfire 4.2.3 Apache2.0, JSoxlibv1.6 (None), Smack 4.2.2 Apache2.0	Yes
Deep Counter	KEIO	Non M-Sec	C, C++	YOLO, SSD, OpenCV	Yes
TST IoT Environmental devices	TST	M-Sec extended	NB-IoT, MQTT	jQuery 3, DataTables, bootstrap v1.2.3, Modernizr.js, Python's standard library 3.4.0, Paho MQTT Python	Yes
TST IoT crowd-counting devices	TST	M-Sec extended	MQTT, GPRS, Java, PHP, SQL	jQuery 3, DataTables, bootstrap v1.2.3, Modernizr.js, Python's standard library 3.4.0, Paho MQTT Python	Yes
Caburn Home Monitoring Devices	External Provider	Non M-Sec	MQTT	Not available	No

The following table provides a summary for each of the results identified above, more specifically:

- Who has the ownership
- Type of Component
- The minimum license (preliminary license) of the code based on the licenses being utilized within the code.

Table 8. M-Sec Core System Components Licenses for exploitable results

Functional Group	Component	Ownership	IP Conditions	License	Public Availability
Development & Security Designing Tools	Security Analysis Tool & Development Method for a secure service (SAT & DMSS)	NII	Proprietary	Under Investigation	TBD
	Modal Transition System Analyser (MTSA)	WU	Proprietary	Under Investigation	TBD
	Node-RED	External tool	FOSS	Apache License 2.0	Yes, https://github.com/node-red/node-red
	Honeypot (IoTPOT)	YNU	Proprietary	NA	No
Secured & Trusted Storage	Crypto Companion Database (CCDB)	WLI	FOSS	MIT License	Yes, https://github.com/jordiescudero/wl-bc-cs/
	Quorum Blockchain & Blockchain Middleware	ICCS	FOSS	Apache License Version 2.0	Yes, https://github.com/jpmorganchase/quorum-examples
	Trust & Reputation Model/Engine	ICCS	FOSS	Apache License Version 2.0	Yes (it will be provided during 3rd Year)

IoT Data Marketplace	IoT Marketplace	ICCS	FOSS	Apache License Version 2.0	Yes (it will be provided during 3rd Year)
	Mobile Wallet	WLI	FOSS	MIT License	Yes, https://github.com/bloomenio/bloomen-wallet
Secure City Data Access	Eclipse sensiNact platform and Studio	CEA	FOSS	Eclipse license	Yes, https://projects.eclipse.org/source-repository-type/git
	Secure SOXFire	KEIO	FOSS	Apache License	Yes, https://www.sfcity.jp/tools/soxfire/?lang=en
Devices Security	Secured components for devices and gateways	CEA	Under investigation	Under investigation	TBD
	Intrusion Detection System (IDS)	YNU	FOSS	OISF/GPLv2 license	No
	Monitoring & Visualisation tool	YNU	FOSS	Elastic/Apache License	No
End to end Security	Security Management Tool	CEA	Under investigation	Under investigation	TBD
Privacy Management	Ganonymizer	KEIO	Proprietary	NA	No

Table 9. M-Sec Pilot System Components Licenses for exploitable results

Component	Ownership	IP Conditions	License	Public Availability

Park Guide	TST	FOSS	GPL	Yes (it will be provided during 3rd Year)
Worldline Connected Care Assistance	WLI	Propietary	NA	No
Smile City Report	KEIO	FOSS	Under investigation	No
Deep Counter	KEIO	Proprietary	NA	No
Secure Mobile Sensing Platform	KEIO	Proprietary	NA	No
TST IoT Environmental devices	TST	Proprietary	NA	No
TST IoT crowd-counting devices	TST	Proprietary	NA	No
Caburn Home Monitoring Devices	External Provider	Proprietary	NA	No

8. Financial Plan & Revenue Models

The challenge for M-sec once the project ends (along with the income stopping) is how to generate funding to cover the operating costs. The obvious target is to move to a payment model. M-Sec investigates various pricing possibilities as presented below. The final price model will be presented on year 3 of the project within the last version of this deliverable "D5.8 - Market Analysis and Exploitation".

According to The Business Model Navigator, 90% of all new business models are not actually new. They are based on 51 existing patterns[40].

Add-on	Freemium	Pay Per Use
Affiliation	From Push to Pull	Pay What you Want
Aikido	Guaranteed Availability	Peer to Peer
Auction	Hidden Revenue	Performance-based Contracting
Barter	Ingredient Branding	Razor and Blade
Cash Machine	Integrator	Rent Instead of Buy
Cross-selling	Layer Player	Revenue Sharing
Crowdfunding	Leverage Customer Data	Reverse Engineering
Crowdsourcing	Licensing	Reverse Innovation
Customer Loyalty	Lock-in	Robin Hood
Digitization	Long Tail	Self-service
Direct Selling	Make More of it	Shop in Shop
E-commerce	Mass Customization	Solution Provider
Experience Selling	No Frills	Subscription
Flat Rate	Open Business	Supermarket
Fractional Ownership	Open Source	Target the Poor
Franchising	Orchestrator	Trash to Cash

Figure 18. Overview Business Models

[40] https://businessmodelnavigator.com/explore

After analysing the different types of Business Models, the consortium may go for the following business model:

- a subscription based business model for data providers to access the M-Sec MarketPlace . This decision has been based on the following analysis:

Table 10. IoT Marketplace Business Models

Name	#IoT Data Marketplace: Commission	#IoT Data Marketplace: Subscription Fee	#IoT Data Marketplace: Pay Per Hour
Description	This is the most common business model deployed by modern Marketplaces. The platform operator imposes either a fixed or variable fee on each successful transaction.	It involves a membership fee, a recurring fee used to charge the users to have access to the Marketplace.	This monetization strategy works for sensor data Marketplaces that sell data streams.
Pros	A commission model attracts both data providers and data consumers, as they do not need to pay anything until they get some value from the Marketplace.	Predictable and recurring revenue stream	Predictable and recurring revenue stream
Cons	It is important to provide enough value to both consumers and providers. If not, there will not be enough numbers of users to maintain Marketplace sustainability.	This model requires users to pay before having access to the Marketplace. An entrance fee is likely to discourage people from joining, especially during the first phase when there are not many users on site.	This model requires users to pay before having access to the Marketplace. An entrance fee is likely to discourage people from joining, especially during the first phase when there are not many users on site.
Existing IoT Marketplaces using the Revenue Model	Microsoft Azure DataMarket.	Qlik DataMarket, Dawex, and QueXopa	IoTA
Viability for M-Sec	Medium	High	Low

- a Freemium Approach (free service for basic functions, premium service for advanced ones) for the M-Sec secure IoT framework with additional paid services for the developer community, such as professional technical support, training and consultancy. The consortium relies on a freemium approach mainly because it offers a good market entry strategy to get users fast and test the viability of the M-Sec offering in the market.

-M-Sec will provide the following services on demand:

- Consultation: Training and consulting services are provided (and paid for) in order to help technology developers to address Security issues
- Integration Support
- Adhoc Development

During the third year of the project, the consortium will detail the different types of subscription model for the M-Sec Marketplace (Corporate Bronze, Silver and Gold) along with the features included on each of the subscription plans as well as the free capabilities offered by the M-Sec IoT Secure Framework and the additional premium features. In order to establish the price and the features, a financial plan will be conducted where future Revenues and Costs will be analysed with the aim of ensuring M-Sec operative sustainability and exploitation.

To implement the freemium model successfully for the M-Sec IoT Secure Framework and the Subscription Model for the Marketplace, during the third year of the project, the consortium will define and describe on the last Market Analysis and Exploitation deliverable (to be submitted on M36) the limitations on certain aspects of the M-Sec Secure IoT Framework.

- **Feature limitations**: Offering extra features, enhanced functionality of available features, or ad hoc paid upgrades (e.g. rare items in a game)
- **Usage quotas:** Storage limits, monthly credits, data processing quotas
- **Limited support:** Tiered access to customer service and support resources

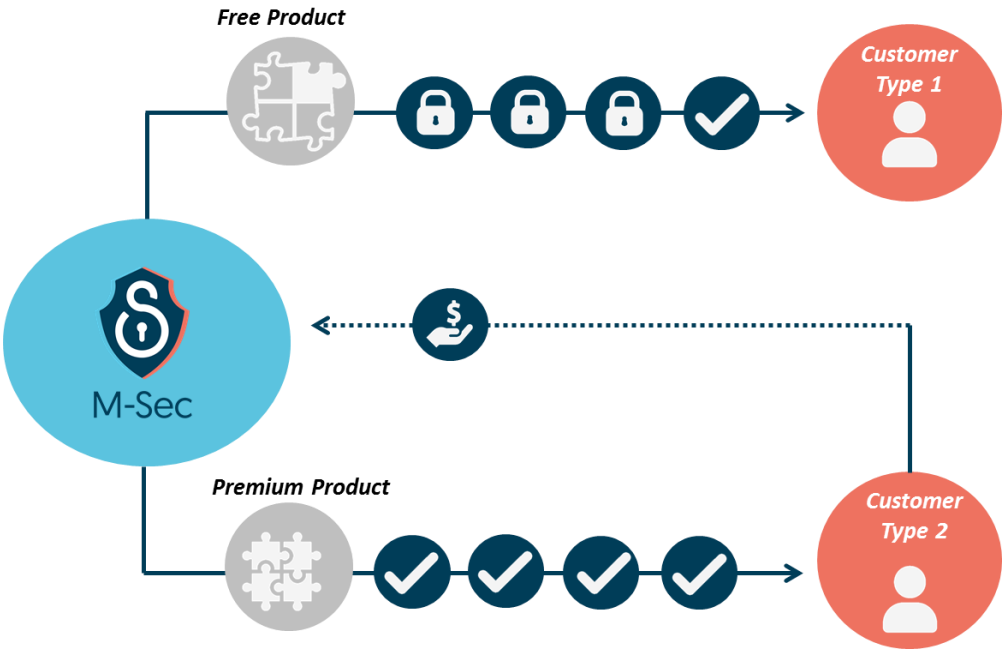

Figure 19. M-Sec Freemium Model

9. Marketing Plan

Most of the content mentioned so far in this document is part of the marketing plan as it addresses what is commonly referenced as “Analysis of the current situation”. This must be a recurrent task as context will evolve and we need to revisit M-Sec positioning. Sources of updates in positioning can be internal as M-Sec will evolve reacting to the way we are satisfying market needs and fulfilling new market needs, or external for example reacting to the entry of new competitors or business models.

At this point in time, considering the stage of M-Sec development it is more useful to reason on the Marketing Funnel Phases and how they can be aligned with M-Sec communication and dissemination activities, in essence, how we can transform project results, outcomes during project implementation, in impact, outcomes of actions after the project ends.

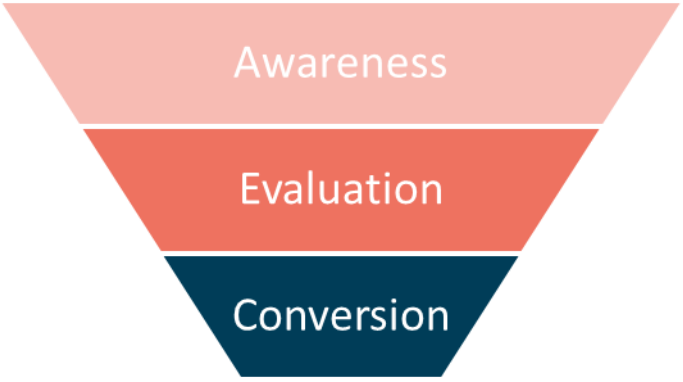

Figure 20 Content marketing funnel

The typical phases of the marketing funnel are: Awareness, Evaluation, Conversion and Delight. During the awareness phase we must assume that potential stakeholders are not aware of neither the consortium nor the solutions we are providing. It is our job to educate potential clients in the challenges they are facing and on potential solutions. In the Evaluation phase, potential clients know that they have a problem and are aware of our solution. It is our job to build trust so that they decide that the **M-Sec framework** is the solution for their challenges. In the conversion phase, potential clients are convinced that our solution is the answer to their challenges and it is our job to provide clear reasons for them to decide that investing on M-Sec is the smart thing to do. Finally, in the delight phase, clients that have bought our solution are invited to provide feedback and generate new content. It is our job to make sure that they are communicating with us providing feedback on M-Sec and referrals to other potential clients.

9.1 Awareness phase

The awareness phase has already started; it is part of the communication and dissemination strategy of M-Sec. We are interacting with cities and citizens to collect their needs and present the goals and the M-Sec framework. We are specifically using the following content types:

- Shareable blog posts with text and infographics on M-Sec website
- Social media posts in twitter, LinkedIn, and YouTube

- Videos for which we have a roadmap.

The evaluation of the effectiveness of the tools implemented if being assessed with communication and dissemination KPIs of the project. However, there are two aspects that need to be revisited. The first is the fact that that the targets of M-Sec communication and dissemination strategy are fully aligned with the stakeholders mapping defined in this document. The second aspect is that the Communication and Dissemination plan of M-Sec is time-bounded to the project duration. The business model canvas as already includes marketing costs in budget specification so we will have resources to reach implement this phase of the funnel after project ends.

9.2 Evaluation phase

As mentioned, the key goal of the evaluation is to build trust in the potential clients. Essentially potential clients need to be confident that:

- they have a problem that needs to be addressed,
- among the multiple options available, the M-Sec framework is the solution.

M-Sec pilots are the kick-off for this phase and the major contributor to build trust across the ecosystem. They already involve representatives of stakeholders identified in the Stakeholder mapping section (5.1) and demonstrate how M-Sec framework is used in 5 use cases scenarios.

In the timeline of M-Sec project implementation, we will be able to produce:

- Case studies documenting the pilots, namely the problems or challenges and how they were addressed
- White papers to documenting challenges and they be solved using M-Sec framework
- Useful resources or downloads, for example scientific papers describing how M-Sec addresses specific needs
- Events and webinars, where the M-Sec project staff addresses multiple perspectives of the project.

In terms of monitoring the success of the methodology we will monitor closely indicators which may reveal:

- Are people converting with this content?
- Is the available content generating new leads or sales?
- Is the content helping or hurting their goals?

9.3 Conversion phase

During this phase, we need to close the deals with the potential clients. By this phase, clients have identified problems or challenges to be addressed, know about the company and the product and we are ready to close the sale.

In order to close the sale, we need to make sure that:

- The digital content has a clear call to action
- The purchase process is as simple as possible

As mentioned in section 8 M-Sec is evaluating different revenue models including freemium ones. The strategy to close the sales will be fine-tuned according to the concrete licensing chosen.

9.4 Delight phase

From the marketing perspective, In the Delight phase we need to engage with existing clients to make sure that they help M-Sec improve the product and bring new clients to the marketing funnel. We need to keep building audience and make sure that they are engaged.

The digital presence of M-Sec needs to make sure that:

- Clients are encouraged to leave feedback
- Publications provide reasons for readers to share and refer to friends
- Contents showcase real customer success

9.5 Relation with business model canvas

This plan is fully aligned with the business model canvas as most of the marketing activities are mentioned in the canvas or the resources are considered there. The first 3 phases; awareness, evaluation and conversion are primarily integrated executed in the context of “Channels” section; Delight is executed in the context of the customer relationships section.

However, the marketing strategy is transversal to the whole business model canvas, it is designed based on the canvas decisions, and the feedback from the marketing activities will provide data to revisit the business model canvas.

10. Conclusions & Next Steps

10.1 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 SotA of technologies employed within the project as well as Market Drivers. In order to identify the M-Sec position in the market, the consortium has performed an extensive analysis on main competitors that covers the same approach on security than M-Sec followed by a SWOT analysis to identify barriers and drivers that will help M-Sec on setting the correct strategy to compete successfully.

Stakeholders are identified and mapped in order to ensure maximum focus and engagement of those ones that are higher interested on the M-Sec project and at the same time may provide a higher impact on the exploitation results of the solution developed by the project.

Additionally, a business model canvas and a value proposition have been developed for the whole M-Sec outcome (IoT Secure Framework and Marketplace) in order to guarantee maximum results in terms of M-Sec exploitation. M-Sec is defined as a product, providing the extensive details on the offering and how the offering covers some of the main challenges found on today's market.

Components generated, enhanced or brought to the project are identified, including a brief description about the component, software libraries used, owner of the asset as well as applicable license.

Finally, an initial draft about the different revenue models for M-Sec is provided along with a Marketing Plan to maximize dissemination and engagement of stakeholders.

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

- Based on the stakeholders analysis provided on section 5, the consortium will manage closely the dissemination activities and engagement on those stakeholders classified with high interest and high influence; Governments and Smart cities and IoT providers (application, cloud, device).
- Based on the competitor's analysis, the SWOT and the Business Model Canvas, M-Sec will be promoted as:
  - End to end security framework covering the whole chain of the IoT ecosystem and validated through five different use cases
  - An open source framework with a freemium model where to experiment on top of it.
  - A Marketplace of IoT Data where to monetize raw data from sensors with new business models
  - An ecosystem with relevant expert partners and stakeholders where to exchange challenges and findings
- In section 7, the IPR for each of the M-Sec components are identified. The consortium has based the assignment of the licenses type on possibly open source license to boost acquisition.
- In terms of revenue models, the consortium relies on a freemium approach mainly because it offers a good market entry strategy to get users fast and test the viability of the M-Sec offering in the market.

- Dissemination activities will be aligned based on the outcomes from this deliverable as it can be seen on section 9 Marketing Plan.

10.2 Next steps

This is a second version of the plan, which will need a future revision, at a later stage of the project, in M36. During the third year of the project, it is expected to have the final financial plan that will be the basis to ensure the sustainability and operation of the M-Sec outcomes after the project's conclusion, as well as the final revenue models. In addition, all the feedback gathered from the point of view of users and stakeholders during pilot trials will be considered for the redefinition of the exploitation plan of M-Sec and the sustainability of the M-Sec framework. Finally, the last deliverable will also include an update of the Business Model Canvas from the different use cases that validate M-Sec.