Multi-layered Security Technologies

for hyper-connected smart cities

D5.9: Community Building Plan

June 2019

Grant Agreement No. 814917

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

Project acronym	M-Sec
Deliverable	D5.9 Community Building Plan
Work Package	WP5
Submission date	28 June 2018
Deliverable lead	F6S/KEIO
Authors	F6S/KEIO/AYTOSAN/WLI/NTTE
Internal reviewer	AYTOSAN/NTTDMC
Dissemination Level	Public
Type of deliverable	R
Version history	- V01, 11/March/2019, F6S, Table of Contents, Full Draft - V02, 18/March/2019, F6S, Table of Contents, Reviewed - V03, 15/May/2019, F6S, Initial Draft - V04, 30/May/2019, F6S, Full Draft - V05, 04/June/2019, WLI, contribution to section 4.6 - V06, 07/June/2019, AYTOSAN, contribution to section 4.2 - V07, 10/June/2019, KEIO, inputs to deliverable - V08, 17/June/2019, AYTOSAN, inputs to deliverable - V09, 18/June/2019, F6S, Final Draft - V10, 24/June/2019, AYTOSAN, WLI, NTTE, final inputs - V11, 27/June/2019, F6S, Final Version

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

Table of Contents

Table of Contents 3

List of Tables 4

List of Figures 4

1. Introduction 5

2. M-Sec community goals 6

3. Target audiences and KPIs 7

4. Facilitation of the community 10

4.1 Communication and dissemination tools 10

4.2 Workshops and events 12

4.3 Community event / online contest 14

4.4 Awareness building activities 14

4.5 Synergies with other initiatives 15

Urban Technology Alliance 15

Regional IoT and Information Force Consortium 17

4.6 Internal Communication mechanisms 18

5. Monitoring and impact 20

6. Conclusions 21

List of Tables

Table 1. M-Sec community target groups 8
Table 2. Assignment of community managers in Europe and Japan 20
Table 3. Partners responsible per pilot 20

List of Figures

Figure 1. M-Sec Smart Cities 7
Figure 2. M-Sec community - discussion between partners 7
Figure 3. M-Sec Newsletter subscription box on the website and first newsletter snapshot 10
Figure 4. Examples of social media posts (promotion of newsletter and sharing blog post) 11
Figure 5. F6S IoT Group snapshot 11
Figure 6. Examples of events with M-Sec participation 12
Figure 7. M-Sec section at the Santander Municipal website 14
Figure 8. Urban Technology Alliance 15
Figure 9. The Urban Technology Alliance launch event in Tokyo, 17-19 December 2018 16
Figure 10. Regional IoT and Information Force Consortium 17
Figure 11. M-Sec partners in project meetings 19

1. Introduction

This document was elaborated for the **M-Sec (Multi-layered Security technologies to ensure hyper-connected smart cities with Blockchain, BigData, Cloud and IoT) project**. It corresponds to the Deliverable 5.9 – Community Building Plan, which is part of Work Package 5: GDPR, dissemination, exploitation and sustainability. WP5 will run from Month 1 until Month 36, i.e. the whole duration of the project.

The M-Sec community is managed under Task 5.4 – Community building and sustainability activities. The sustainability activities described in D5.6 will contribute to maintaining and growing the M-Sec community after the project ends.

This report describes the nature of the community that will be built for M-Sec and the plan with the appropriate measures for realising this community. After this Introduction, the report is divided in the following sections:

- Chapter 2 presents the goals for the M-Sec community;
- Chapter 3 presents the target audiences of the M-Sec community, as well as presents how the project will engage with them. Such engagement will be monitored with a set of KPIs;
- Chapter 4 describes the different activities to build and facilitate the community, including communication and dissemination tools, workshops and events, online contest, awareness building activities, and synergies with other initiatives;
- Chapter 5 identifies the community managers and pilots representatives, and how the community will be monitored and assessed;
- Chapter 6 provides the conclusions of this report.

2. M-Sec community goals

The aim of the M-Sec community is to facilitate interaction and create of synergies between the stakeholders that are involved in, and have an interest in, the project. It is expected that the community is based on shared interests in connecting EU and Japan ecosystems, in improving the security of IoT, big data, cloud, blockchain technologies and, in principle, that it supports putting in place exploitation activities that open up M-Sec to other contexts and geographies. The M-Sec Task 5.4 - Community building and sustainability activities, is led by F6S on the EU side, and KEIO on the Japanese side.

The following goals are important for the M-Sec community:

- **To promote the participation of the community members in the project activities and events:**
  The activities to be put in place will help in mobilising potential users of the solutions, both within the scope of, and beyond, the project pilots. Indeed, it is important to encourage relevant stakeholders to co-develop the solutions and continuously participate in the project activities. By creating a set of tools and communication channels, both online and offline, M-Sec fosters a close contact and active communication between community members. It not only promotes their active participation in the M-Sec pilots, giving them a sense of being part of a greater cause, but also fosters the exchange of knowledge and sharing of research results, resulting in win-win collaborations.
- **To provide a regular and efficient internal communication:**
  The M-Sec consortium consists of a partnership between 12 European and Japanese organisations, with multiple researchers and project managers. Internal communication procedures have been defined under WP1 and are presented in section 4. This helps ensuring that all partners are aligned with the project developments and results, reflecting the knowledge and dynamics of each use case, and supports a wider engagement of the M-Sec community.
- **To serve the community with high-quality project results:**
  The project results to be disseminated to the M-Sec community have been outline in Deliverable D5.2 – Initial Dissemination Plan (see Table 3 – Key M-Sec elements and public deliverables to be disseminated). In total, M-Sec will produce 40 deliverables, of which 33 will be made public (as well as all technical deliverables). Depending on the submission date and approval by the European Commission, a strategy for planning the content and disseminating the results will be put in place, consisting of a set of activities: from publication in the project website, development of blog posts and interviews with the responsible partners, as well as release in the periodic newsletter.
- **To establish synergies with relevant initiatives and support the M-Sec sustainability:**
  As mentioned above, the M-Sec community will be built around common interests, to support the exploitation and sustainability of the project results. It is thus critical to establish collaborations with relevant organisations, projects and initiatives. An exercise to identify similar initiatives and solutions in the market has been put in place within the Exploitation Task (see D5.6 - Market Analysis and Exploitation - first year report). Under WP5, M-Sec has initiated contact with relevant initiatives, as presented in detail in D5.2, D5.3 and briefly described in section 4 of this report. At the initial stage of the project, the collaboration is focused on cross promotion of activities. When research results will be published, further ties will be explored by the technical partners.

3. Target audiences and KPIs

This section describes the target audiences to be addressed. The members of M-Sec community include the following types of stakeholders, also described in D5.2 – Initial Dissemination Plan:

- **General public (including industry and SMEs);**
- **Research community;**
- **Standards and regulation bodies;**
- **Cities field trial stakeholders / community (including citizens);**
- **Innovators (startups, developers);**
- **EU-Japan initiatives and policy makers.**

It is important to notice that when referring to each target audience, M-Sec is considering the stakeholders in the 2 smart cities of the project, as well as actors around the EU and Japan.

Fujisawa

Santander

Figure 1. M-Sec Smart Cities

During the 2nd Face-to-Face meeting in Fujisawa, April 2019, a brainstorming exercise was conducted among all partners, to better assess the needs of these stakeholders, how the M-Sec solutions can help addressing such needs, and how to best reach out to these audiences. The results of this activity are provided below, setting the scene for facilitating the M-Sec community. The KPIs to measure the approach to each target audience have been revisited and are presented below as well.

Figure 2. M-Sec community - discussion between partners

Table 1. M-Sec community target groups

	Needs *What is the problem?*	M-Sec Solutions *What does M-Sec provide?*	Outreach *How to reach this stakeholder?*	Communication KPIs *How to measure the approach?*
General public (including industry and SMEs)	- SMEs have difficulty with access to the market, mainly due to the complexity of city organisations; - Data privacy, digital trust and public acceptance (how to motivate users to provide data), utility of the data, how to motivate users to provide data.	- Provide a marketplace (through Use Case 5 – A marketplace of IoT services for effective decision making); - M-Sec Security Layers can solve the barriers; – Help users feeling secure, making use of the KPIs regarding security.	- Events to catch potential customers, workshops to show demos, collaboration between companies, cities and universities	○ 15 Non-scientific publications (articles, press releases, …) ○ 4 Newsletters ○ 3000 Video views ○ >500 Followers in social networks ○ 200 Number of deliverables downloaded ○ 2 Booths in exhibitions
Research community	- Lack of datasets for evaluation of proposed solutions; - Lack of infrastructures and experimental data to test their results; - Implementation issue.	- M-Sec can provide datasets and give data to researchers (limited access for research purposes, and with care of GDPR and consent of users); - Help define benchmarks or criteria so researchers could compare their approaches. Part of the tools and solutions provided should be open source.	- Access to implementations of proposed /published methods - Publish software as open source in Github (part of tools, etc.), with acknowledgement to M-Sec papers - Direct contact with research teams and universities, through papers, workshops, scientific publications - Add datasets to well-known sites (e.g. security repositories)	○ 15 [incl. 5 joint (EU/JP)] Publications in international conferences ○ 3 Publications in international journals ○ 2 Co-organized international workshops
Standards and regulation bodies	- There are too many different types of solutions in the market; - There is a conflict between security needs and market needs (businesses), and different stakeholders' requirements; - End-user considerations	- M-Sec architecture can provide a decentralised platform where there is no single point of failure; - Our solutions can be applied globally as no single controller and developers can get onto the marketplace by following basic security guidelines; - End-to-end security solutions	- With valid trial results and solutions it is easier to raise the awareness of the project results; - Awareness through public dissemination of activities.	○ >3 Standardization groups that project interact with ○ 4 Participations in EU commission's consultation and other worldwide regulatory in the field of interest

	Needs *What is the problem?*	M-Sec Solutions *What does M-Sec provide?*	Outreach *How to reach this stakeholder?*	Communication KPIs *How to measure the approach?*
		provide trust for consumers/end-users. E.g.: Decentralised vs decentralised allows flexibility to evolve echo systems, there is a single interface to connect to marketplace.		
Cities field trial stakeholders / community (including citizens)	- Motivation of the citizens to participate in the field trials; - Security of the data collected, and the use of personal data; - Understand the effects and benefits of the field trials; - Budget after the trial.	- Citizens can contribute to the co-creation of the services in their cities; - M-Sec can provide security solutions to secure the data; - M-Sec can provide successful and concrete use cases with the project results.	- Engage with cities decision makers; - Provide a potential incentive; - Participate in events targeting local governments; - Website information; - Research cities' interests online and directly talking to them; - Participate in alliances (e.g. UTA).	○ 10 Training and community events co-organized (webinars, workshops, hackathons, etc.) ○ 1000 EU/JP Citizens for e-consultation ○ Use case replication in 2 cities or more
Innovators (startups, developers)	- Interested in developing new solutions and products. - Lack of data to develop new products; - Looking for APIs to connect with (Architecture) - In need of security modules – software, hardware, data	- M-Sec pilots show how the integrated platform can be used; - Data, API's and modules to connect with would be relevant but it is not clear whether the project will have these. - Online competition or hackathon with involvement of the cities.	- Connecting with SME clusters; - Participate in smart cities networks, events and startup events - Organise online competition providing testbeds (in Japan and in the EU) as a prize.	○ 1 Online contest with participation of more than 20 startups and entrepreneurs
EU-Japan initiatives and policy makers	- Politicians need more votes and to know citizens' needs; - Policy-makers seek cost-cut opportunities and are concerned with how to use budget effectively. - They need to convince citizens that they are carrying out the right actions and being compliant with GDPR, etc.	- It is important to provide politicians with a framework for citizens involvement. With a citizen involvement app, citizens can confirm that city's strategy/action is based on the policy and based on this sensing.	Ask directly the politicians and present the solutions, e.g. seeking support by Mr. Fukuda (Fujisawa).	○ >4 Participations to EU's concertation activities ○ >4 Joint events with other EU-Japan projects ○ >3 Invitations from governmental institution (embassy, etc.)

4. Facilitation of the community

This section provides a description of the measures and tools to create and facilitate the community:

- Communication and dissemination tools (project website, project news, online platform);
- Workshops and events;
- Online contest;
- Awareness building activities;
- Internal communication mechanisms.

4.1 Communication and dissemination tools

M-Sec uses various communication and dissemination tools, which are described in D5.2 – Initial Dissemination Plan, and D5.3 – Dissemination Activities Report – first year. In this subsection, the tools that help fostering the M-Sec community are briefly presented.

Project website

The project website (www.msecproject.eu) concentrates on all the information about the M-Sec activities, as well as provides easy access to the project results. The menu includes a section called "Resources", which has been carefully designed for the M-Sec stakeholders, by providing the following: the online M-Sec media kit, relevant initiatives, scientific papers, deliverables, how to get involved (to learn how to get involved in the project activities) and press coverage. Moreover, external stakeholders can interact with M-Sec via the project website by using the contact form in "Contact", and by signing up to the M-Sec newsletter.

Project news

Apart from the newsletter mentioned above, which presents official project news regularly, external stakeholders can access project news by reading the blog posts and press releases on the website, as well as quick project updates visa social media: M-Sec on Twitter - @MSecProject, and on LinkedIn - M-Sec Project.

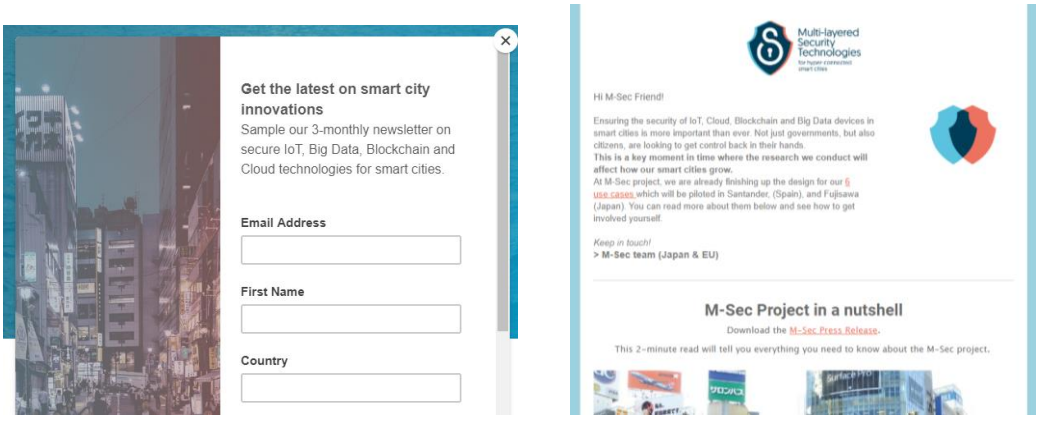


Figure 3. M-Sec Newsletter subscription box on the website and first newsletter snapshot

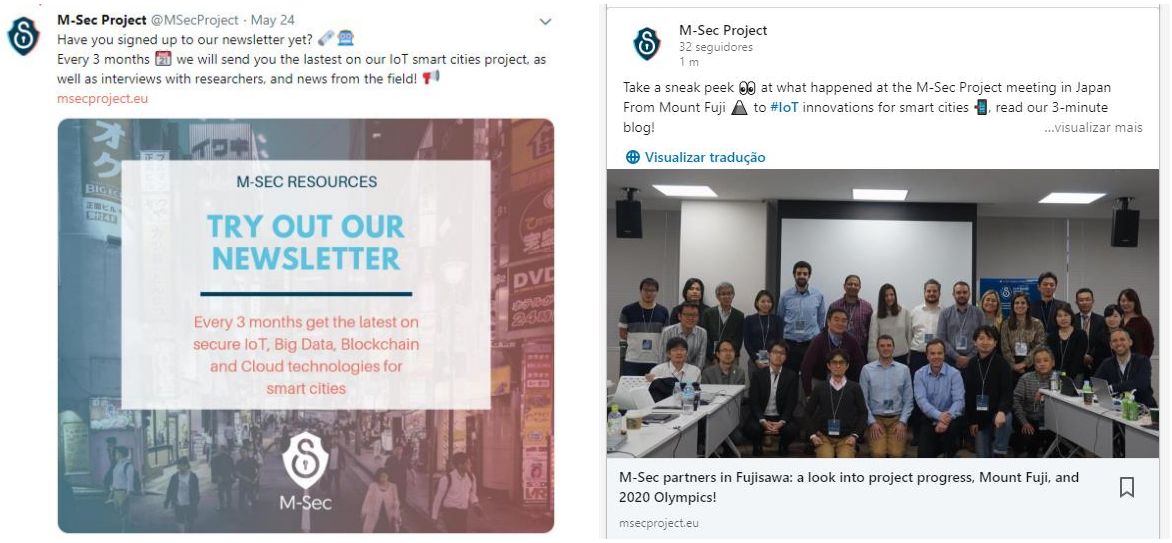


Figure 4. Examples of social media posts (promotion of newsletter and sharing blog post)

Online platform – open discussion group

In addition, the M-Sec Community will be facilitated through an online platform, where consortium partners and relevant stakeholders can post, exchange information and interact with each other. This group is available on F6S and gathers a community of 9,544 SMEs and startups interested in the topic of Internet of Things. M-Sec stakeholders can sign up for free to M-Sec and join the group though www.f6s.com/iot.

Once project results are available, these will be communicated in the platform, thus engaging with relevant stakeholders all over the world. The platform will also facilitate the engagement with innovators and entrepreneurs at a later stage in the project.

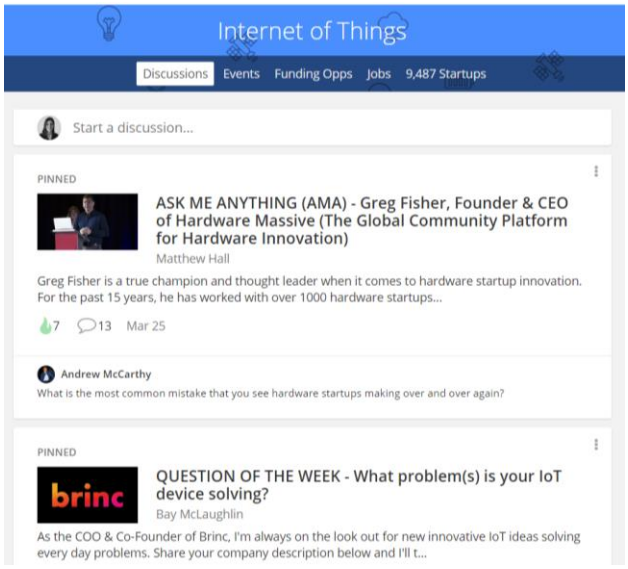


Figure 5. F6S IoT Group snapshot

4.2 Workshops and events

M-Sec will organise its own events, hereby designated internal events, as well as actively participate in external events from other initiatives and scientific conferences. Below is a description of the upcoming plans for the organisation of workshops and participation in events.

Worldline and CEA present M-Sec in "EU, Japan and Korea collaboration for breakthrough innovation" workshop in ICT 2018, Vienna, 4 December 2018

Ayuntamiento de Santander - Presentation of M-Sec in Almada Import Workshop, 29 May 2019

Figure 6. Examples of events with M-Sec participation

Internal events

As described in D2.2, the project will mostly interact with its community during the pilots. Indeed, the facilitation of the M-Sec community will also be achieved through the organisation and invitation for **workshops and events** relevant to the ecosystem; and respective follow-up/ dissemination among peers.

It is expected that M-Sec organises minimum 10 training and community events, ranging from webinars, workshops and hackathons, each one addressing between 20 to 50 participants. In addition, it is expected that 1000 EU/JP citizens participate in the M-Sec consultation, and that at the end of the project the use cases will be replicated in 2 additional cities or more.

Upcoming citizen engagement activities in Santander

Firstly, it is important to involve the municipal services, as the best connoisseurs of the operation of the service as well as the local stakeholders involved. Therefore, meetings have been held with responsible for municipal services and councillors, belonging to the environmental service, social services, education and the local development agency. In these meetings, after a presentation of the M-Sec project, pilot experiences to be carried out were discussed, identifying potential stakeholders and how to reach them.

Based on the experience in other European projects, it is more efficient to start the engagement of a small number of users, called friend users, who may provide their feedback and test M-Sec solutions. Therefore, an initial workshop will be organised in order to present M-Sec project and pilots to be carried out, with the aim of attracting them to participate. Workshops' attendees will be chosen in collaboration with the municipal services. Taking into account the planning included in Deliverable 2.2, this initial workshop should

be held between September & December 2019 (Month 15 - Month 18) in order to engage the stakeholders of Pilots 1.1, 1.2, 2.1, 2.2, 5 and 6.

At least one workshop per year and use case will be organized during the second and third years of the project, with the aim of attracting more users. When the testing stage has passed, M-Sec solutions will be promoted more widely, through local media channels reachable by the consortium members, including the municipal ones, such as the municipal website. Additionally, and in order to give greater visibility and dissemination to M-Sec pilots, it would be possible to participate in some of the events organized by the municipal services. For example, M-Sec will likely take advantage of an event organized by the environmental service to promote the pilots to be developed in the Llamas park.

Pilot 2.1 requires a special mention because due to its target audience, elderly users of telecare service, it is not possible to organize a single workshop attended by all potential participants. In this case and in collaboration with representatives of Social Care Service, a dedicated meeting with each potential friend user and their family member or neighbour will be organised, in order to present them the pilot and invite them to be participants.

Upcoming citizen engagement activities in Fujisawa

Three workshops are planned in 2019, to engage the stakeholders of Pilots 3.1, 4.1 and 4.2, and 5. In particular, the workshop for Pilot 3.1 invites the local government officers and industry workers that are responsible for garbage collection in Fujisawa city. The participants are requested to understand the functionality of the M-Sec architecture and the service used in the Pilot. The workshop will last for about 1 hour and will include lectures by KEIO and a question/answer session. Similar workshops will be held for the other pilots inviting local community members, such as children, the elderly, and other citizens. The invitation will be made in collaboration with Fujisawa city to attract more people. In the first half of the year 2020, three similar workshops are planned. After the first workshops for those pilots, the second ones will be more focused on the practical use of the applications and the services evaluated in the pilots. Further details are provided in the activities of WP2.

External events

From the start of the project, M-Sec partners actively engage with policy makers and the research community during events and conferences. A plan for the participation in such events is commonly shared between partners, and participation in future events is guaranteed, where scientific results will be presented and discussed. A considerate number of relevant events have been attended by the M-Sec project partners in the first year of the project. All details about the participation in events is provided in Deliverable 5.3 – Dissemination Activities Report – first year.

During the second year of the project, it is expected that the M-Sec partners will participate in more events and to more extensive level, mainly because the first results/prototypes of the project will be available. In addition to participating in different forums in which Santander City Council presents innovation city initiatives along with pilot experiences from European projects, the Municipality also hosts delegations from different parts of the world interested in its strategy as a Smart city, being both good opportunities to promote the project.

4.3 Community event / online contest

The organisation of a community event / competition with innovators and developers is planned for Month 20 of the project. By launching an online contest, M-Sec will be able to engage industrial and academic sectors towards the adoption and or development of the project findings.

Such a contest should be focused on solving IoT challenges and providing solutions for smart cities. The contest should have the participation of more than 20 startups and entrepreneurs, who would apply by demonstrating how their solutions could help solving the challenges presented by the cities.

As a prize or incentive, the online competition could provide testbeds in Japan and in the EU, offer travel and accommodation for selected innovators, and arrange meetings/presentations of the solutions to relevant audiences and decision makers in Fujisawa and Santander.

4.4 Awareness building activities

Awareness building activities will be implemented in both Fujisawa and Santander to support citizen engagement and community animation.

In Fujisawa, NTTE will explore the engagement of stakeholders in the project activities to obtain research cooperation. Specifically, the project will approach organisations by investigating the relevance to cooperate with cities, while describing meaningful use cases for the utilisation of project results.

Santander municipal website includes a section for European projects in which the municipality participates, such as M-Sec (http://santander.es/content/m-sec-disenando-ciudades-inteligentes-del-futuro). Besides including a link to the official project website and the Spanish version of news and newsletters, the content will be updated as the project progresses, so that citizens can follow its evolution and it is also easier to recruit new users, as a complement to the workshops and events described in section 4.2.

Figure 7. M-Sec section at the Santander Municipal website

4.5 Synergies with other initiatives

By establishing synergies with the academic sector, other relevant initiatives and standardisation bodies, M-Sec will further promote the project activities and results and engage with its community members. A strategy on engaging with such organisations has been created and has been presented in D5.2 and D5.3, including how to formalise connections in the future. M-Sec will engage with such initiatives, exchange knowledge and results, invite members to the project activities, as well as build communities together.

Initiatives to collaborate with include IoT European Research Cluster, OSGi Alliance, Fiware, XMP Foundation, among others. In addition, relevant EU-JP collaboration projects and smart city intiatives are also relevant to cooperate with. These have been identified within Task 5.2 Exploitation and IPR activities, and are presented in D5.6 Market Analysis and Exploitation (updated every year). Examples include Waltonchain, Chariot, Brain-IoT, Decenter, and others.

To better explain the activities which will be implemented within the collaboration with other initiatives, the synergies with 2 relevant organisations are demonstrated below: Urban Technology Alliance; and Regional IoT and Information Force Consortium.

Urban Technology Alliance

Urban Technology Alliance - http://www.urbantechnologyalliance.org/

The Urban Technology Alliance (UTA) is a global non-profit organization providing city-scale testbeds from all around the world, to deploy, test and validate the latest smart city innovations. The UTA is providing trusted and neutral guidance to cities for their sustainable digital transformation, enabling them to face today's economic, social and environmental challenges. The UTA is a vibrant community including a smart city ecosystem composed of cities, industry, academy and non-profit organizations.

UTA members network, build partnerships, deploy and test concrete solutions in real-life environments and share best practice and success stories among members worldwide.

5 Working Groups: Technical, Business, Sustainability, Testbed, Social

What does UTA deliver?

- Organizes pilot deployments and trials in the member cities for proof of concept validation
  - Share best-practices, success stories, business cases, lessons learnt, evaluation studies and testbed reports within the UTA community
- Provides technical and non-technical guidelines and methodology for implementing trials
  - Recommends reference architectures, integration plans, standards, KPIs and sustainability metrics
- Builds a technology/community agnostic marketplace, create strategic partnerships
  - Provides a one-stop showcase of smart city solutions

Figure 8. Urban Technology Alliance

There are multiple activities of smart city projects existing worldwide. However, most of them are individual activities, which means there is no existing “one place” for sharing not only technologies but also solutions, data, know-how, etc. which originate not only from the developing side (big corporates, SME, R&D labs) but also from city offices, citizen, tourists, etc.

According to a study from Machina Research, now part of Gartner (an M2M and IoT research firm), cities worldwide could waste as much as $341bn by 2025 if they adopt a fragmented approach towards IoT as opposed to a standardised one. From the technical viewpoint, of course, there are already several activities building IoT platforms as ecosystems, but another important issue is that there are so many IoT platform existing that users have difficulty understanding which solution they should adopt.

According to the research firm IoT Analytics, there are more than 360 different IoT platforms available worldwide. Of this number, more than 60 are targeted specifically at the smart city.

From these backgrounds, and as an important result achieved by several international H2020 projects (BigClouT, ClouT, BigClouT, FESTIVAL, Wise-IoT, as well as IoT-EPI CSA project, Unify-IoT), a global initiative has been established: Urban Technology Alliance (UTA). As some of the M-Sec partners are engaged in UTA, a strong collaboration is foreseen between the M-Sec community and the UTA activities.

As a first step in the collaboration, M-Sec project partners participated in the Urban Technology Alliance launch event, which took place in Tokyo, 17-19 December 2018. The event participants included UTA members and honourable guests, who presented the city testbeds and project solutions to an audience of 120 attendees.

Figure 9. The Urban Technology Alliance launch event in Tokyo, 17-19 December 2018

Regional IoT and Information Force Consortium

Regional IoT and Information Force Consortium - https://www.kri.sfc.keio.ac.jp/en/consortium/riot/

The consortium aims to promote the research and education listed below with the goal of creating a smart city through industry-government-academia cooperation. By doing so, SFC will be established as an international smart city center of excellence. A cooperative agreement has been signed between the SFC and Fujisawa City in Kanagawa Prefecture, and based on this agreement the Laboratory Representative is currently cooperating with the City to promote several projects regarding smart cities.

4 Working groups: Utilisation of public vehicles, Participatory sensing, Smart Mobility, Local government live data

What does the consortium deliver?

- Organizes pilot deployments and trials of an IoT-related technology in the member cities for proof of concept validation
  - Share best-practices, success stories, business cases, lessons learnt, evaluation studies and testbed reports within the consortium
- Provides technical assets owned by member companies for trials of the IoT-related technology and also its future realization
  - Establish practical use cases of the IoT-related technology being connected with those technical assets
- Evaluate the IoT-related technology from differing points of view: local government, industry, and academia
  - Provides requests and comments for the evaluated technology

Figure 10. Regional IoT and Information Force Consortium

The Regional IoT and Information Force Consortium has been building a set of potential IoT, Big Data, Blockchain, and Marketplace applications. This knowledge is beneficial for analyzing requirements and risks inherent in the M-Sec architecture at its development phase. Various members of the consortium, from academia, industry, and local government, can help conducting the M-Sec field studies and trials.

Currently, Fujisawa city (one of the core members of the consortium) is helping to prepare Pilots 3, 4, and 5. Other cities, including Yokosuka, Kamakura, Chigasaki, Sagamihara, Samukawa, and Oiso, have other local issues, such as aging, unoccupied housing, and local community maintenance. These issues, when introduced to M-Sec, will offer opportunities for potential target applications and services of M-Sec architecture. Also, the consortium would be able to host trials and pilots in those cities, which will be a great opportunity for disseminating the architecture.

4.6 Internal Communication mechanisms

For the smooth running of the M-Sec community, it is very important that the M-Sec team (an internal community of 12 European and Japanese organisations) communicates and shares information easily and regularly.

The internal communication procedures, set under WP1 and supported by Task 5.4, include the following:

- **Monthly General Assembly conference calls**

Teleconferences are the most convenient way for partners to meet without spending time and budget on travelling. Since the project started, a conference call has taken place between European and Japanese partners every month.

- **Regular WP conference calls**

In addition to the online General Assembly meetings, teleconferences can be set up whenever necessary, either on the spot or on a regular basis. For instance, a bi-monthly conference call has been set up for WP4 "Multi-layered Security Technologies" in order to achieve the successful demonstration milestone, set for M18 (December 2019).

Furthermore, several calls have taken place during the length of the project to discuss use case and pilot implementation and even to show the appropriate methodologies for the co-creation of a Business Model Canvas for each of the use cases.

- **Periodic face-to-face meetings**

For the M-Sec project, there are two General Assembly meetings per year. One of these meetings takes place in Europe and the other in Japan. In addition, review meetings take place annually so that EU and NICT can assess the progress and achievements of the project. If necessary, extraordinary meetings can be organized during the year.

- **Ad hoc social activities and ice breakers**

As partners are working on a collaborative project at a distance and with different cultures, face to face contact is limited to the periodic face-to-face meetings (maximum twice a year). It is thus recommended that short interactive activities are programmed, to foster the spirit of teamwork and cooperation. These activities can take the form of moderated funny ice breakers at the beginning of a face to face meeting or of social events in the evenings or end of meetings. Such commitment will help partners trust and know each other better, as well as understand the colleagues' backgrounds and scientific interests more easily, thus supporting communication and collaboration.

For instance, after the first Face-to-Face meeting held in Barcelona in 2018, partners were invited to a 1,5h walking guided tour through the Barcelona Old Town and Gothic Quarter. In the same way, after the second Face-to-Face meeting organized in Fujisawa in 2019, partners joined a walking tour through Enoshima, a small island close to Fujisawa. Both social activities helped partners to know each other better while at the same time promote cooperation and strengthen the relationships between all members of the consortium.

- **Regular sharing of information via Confluence management tool**

The M-Sec collaborative workspace is based on Atlassian Confluence, available on

https://www.atlassian.com/software/confluence.

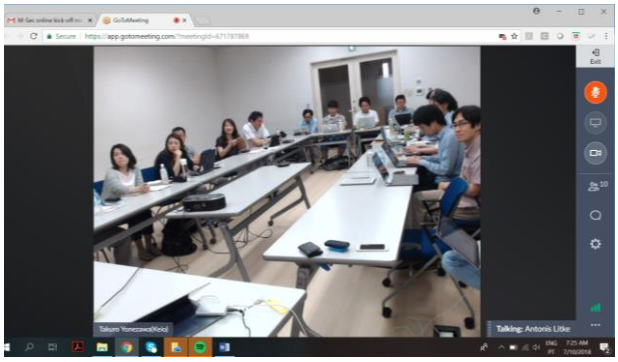
This is not just a document repository, but a powerful tool for teamwork, providing many useful features such as meeting notes, project plans, product requirements, multimedia, and dynamic content, as well as allowing partners to give feedback on the work itself (via inline, page and file comments).

- **Mailing lists**

Given the nature of M-Sec project, with a Japanese consortium and a European consortium working together, offline communications are of remarkable importance. Hence, mailing lists and e-mail are one of the main means of interpersonal communication in M-Sec. Three mailing lists have already been set-up to address different audiences in the M-Sec project: a general mailing list for all partners, a European mailing list and a Japanese mailing list. If required, more mailing lists may be set-up during the project.

- **Dissemination activities**

Finally, all partners have access to the project newsletter and all dissemination activities and communication channels presented in D5.2 and in section 4 of this document serve the consortium as well.



M-Sec Online Kick-Off Meeting, July 2018

M-Sec Plenary Meeting in Barcelona, October 2018

Figure 11. M-Sec partners in project meetings

5. Monitoring and impact

Within Task 5.4, partners will monitor the community and its impact. The metrics presented in section 3 will be used to evaluate and measure the success of the M-Sec community. An assessment has been provided for the status at Month 12. Indeed, the KPIs set for the communication and dissemination activities will support the project team in understanding the progress of engagement in the M-Sec activities and results by the community members.

The Community Building Plan will be revisited regularly, especially during consortium meetings, to guarantee the continuous improvement of the activities implemented to foster engagement and participation.

All project partners have efforts allocated to facilitate the M-Sec community (except for CEA). In addition, the project has assigned community managers in Europe and Japan, who are responsible for animating the community members to take part in the project activities.

Table 2. Assignment of community managers in Europe and Japan

Community Manager: EU side	Community Manager: JP side
F6s, with support by AYTOSAN	KEIO, with support by NTTE

In addition to the community managers, the partner responsible for each M-Sec pilot acts as a representative of M-Sec when engaging with the participants and end users. Their contact and organisation details will be provided in the description of the use cases in the project website, to facilitate enrolment in the project activities, as well as interaction with external entities, thus leveraging other synergies and collaborations. Later on, when project results are released, it will also be assessed if it is relevant to assign project ambassadors to specific technologies used in the project.

Table 3. Partners responsible per pilot

Use cases	Pilot (s)	Pilot's names	City	Partner responsible
1	Pilot 1.1 Pilot 1.2	Reliable IoT environmental data devices with multi-layered security for a smart city Reliable IoT crowd counting data devices with multi-layered security for a smart city	Santander Santander	TST
2	Pilot 2.1 Pilot 2.2	Home Activity Tele-assistance Social & Physical Wellbeing	Santander Santander	WLI
3	Pilot 3.1	Secure Mobile Environment Sensing	Fujisawa	KEIO
4	Pilot 4.1 Pilot 4.2	Privacy-secure Garbage Counting Secure Affective Participatory Sensing of City Events	Fujisawa Fujisawa	KEIO
5	Pilot 5.1	A marketplace of IoT services for effective decision making	Fujisawa & Santander	NTTE
6	Pilot 6.1	Citizen as sensor	Santander & Fujisawa	TST

6. Conclusions

The M-Sec community is managed under Task 5.4 – Community building and sustainability activities, although it is clear that the efforts within Task 5.1 – Dissemination and Communication activities, will have a strong impact in growing the community as well. The M-Sec Community Building Plan outlines the framework for establishing and facilitating the project community, describing the measures to be put in place.

This report begins with an understanding of the goals for the community, to support the scope of the activities to be implemented. Afterwards, it provides an assessment of the M-Sec target audiences [General public (including industry and SMEs); Research community; Standards and regulation bodies; Cities field trial stakeholders / community (including citizens); Innovators (startups, developers); EU-Japan initiatives and policy makers], and presents the KPIs which help measuring the approach towards each target group.

Afterwards, the document describes several activities which will be implemented in order to facilitate the community, ranging from communication and dissemination tools and actions, workshops and events, awareness building activities, synergies with other initiatives, and procedures to support internal communication within the project consortium (inner circle of the M-Sec community).

Finally, the plan details the community managers in the EU and Japan and representatives per pilot, and explains how the community will be monitored and its impact assessed with the support of the KPI frame. During the course of the project, this plan will be visited regularly, especially during plenary meetings.