



# Multi-layered Security Technologies

for hyper-connected  
smart cities

D5.2: Initial Dissemination Plan

December 2018



## Grant Agreement No. 814917

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

<b>Project acronym</b>	M-Sec
<b>Deliverable</b>	D5.2 Initial Dissemination Plan
<b>Work Package</b>	WP5
<b>Submission date</b>	December 2018
<b>Deliverable lead</b>	F6S / NTTE
<b>Authors</b>	Sofia Esteves, Charlotte Tucker, Nuno Varandas – F6S; NTTE; All partners
<b>Internal reviewer</b>	CEA, NTTDMC
<b>Dissemination Level</b>	Public
<b>Type of deliverable</b>	Report
<b>Version history</b>	<ul style="list-style-type: none"><li>- V01, 19/November/2018, F6S, Content, Full Draft</li><li>- V02, 22/November/2018, NTTDMC, Review, Reviewed</li><li>- V03, 19/December/2018, F6S, Adopted review changes, Final</li></ul>

Worldline



TST



YNU



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





# Table of Contents

Table of Contents .....	3
List of Figures.....	4
List of Tables.....	4
1. Introduction .....	5
2. Target audiences.....	7
3. Key messages.....	9
4. Communication tools and channels .....	12
4.1 Visual Identity.....	12
Project name.....	12
Logo and project colours .....	12
Funding information .....	13
Branded templates .....	13
4.2 Project website.....	14
4.3 Social media.....	15
M-Sec channels.....	15
Partners' social media channels .....	16
4.4 News and articles .....	16
4.5 Promotional materials .....	17
4.6 Events .....	19
4.7 Scientific publications.....	20
4.8 Other channels .....	20
4.9 Synergies with other initiatives and standardisation efforts .....	20
EU projects and smart city initiatives .....	20
Standardization bodies .....	21
5. Action Plan .....	23
5.1 Partner responsibilities.....	23
5.2 Communication timeline .....	24



5.3	Partners' channels .....	25
6.	Monitoring and evaluation .....	27
6.1	Communication KPIs.....	27
6.2	Communication reporting .....	28
7.	In a nutshell.....	29

## List of Figures

Figure 1.	Shield shape added for security, and multiple layers were added for a feeling of triple strength....	12
Figure 2.	New M-Sec colour palette for trust and security .....	12
Figure 3.	Example of M-Sec logos and visual identity .....	13
Figure 4.	Example of M-Sec Power Point Template .....	13
Figure 5.	M-Sec project website - homepage screenshots (in English and Japanese) .....	14
Figure 6.	M-Sec Twitter screenshot (November 2018) .....	15
Figure 7.	M-Sec Visual Identity for promotional materials .....	17
Figure 8.	M-Sec smart city .....	17
Figure 9.	M-Sec Project Flyer/Postcard .....	18
Figure 10.	Communication timeline .....	24

## List of Tables

Table 1.	Communication, Dissemination and Exploitation definitions .....	5
Table 2.	M-Sec target audiences .....	7
Table 3.	Key M-Sec elements and public deliverables to be disseminated.....	9
Table 4.	Planned attendance to relevant events in the first 12 months.....	19
Table 5.	Planned standardisation efforts .....	21
Table 6.	Partners' communication channels .....	25
Table 7.	M-Sec dissemination and communication indicators.....	27



# 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 5.2 – Initial Dissemination 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.

## What do “communication” and “dissemination” mean?

In an effort to boost the communication and dissemination efforts M-Sec, it is important to refresh one’s understanding of the terms “communication”, “dissemination” and “exploitation” in relation to H2020 projects. The table below (from the European IPR Helpdesk document “Making the most of your H2020 project: Boosting the impact of your project through effective communication, dissemination and exploitation”,<sup>1</sup> with definitions from EC Research & Innovation Participant Portal Glossary/Reference Terms), outlines the difference between each term and affords an understanding of how to apply this to M-Sec.

**Table 1. Communication, Dissemination and Exploitation definitions**

Communication	Dissemination	Exploitation	
<b>“Communication of projects is a strategically planned process that starts at the outset of the action and continues throughout its entire lifetime, aimed at promoting the action and its results. It requires strategic and targeted measures for communicating about (i) the action and (ii) its results to a multitude of audiences, including the media and the public and possibly engaging in a two-way exchange.”</b>	<b>“The public disclosure of the results by any appropriate means (other than resulting from protecting or exploiting the results), including by scientific publications in any medium.”</b>	<b>“The utilisation of results in further research activities other than those covered by the action concerned, or in developing, creating and marketing a product or process, or in creating and providing a service, or in standardisation activities.”</b>	<b>Definition</b>
<b>Reach out to society and show the impact and benefits of EU-funded R&amp;I activities, e.g. by</b>	<b>Transfer knowledge &amp; results with the aim to enable others to use and take up results, thus</b>	<b>Effectively use project results through scientific, economic, political or societal exploitation</b>	<b>Objective</b>

<sup>1</sup> Available at [https://www.iprhelpdesk.eu/sites/default/files/EU-IPR-Brochure-Boosting-Impact-C-D-E\\_0.pdf](https://www.iprhelpdesk.eu/sites/default/files/EU-IPR-Brochure-Boosting-Impact-C-D-E_0.pdf)







addressing and providing possible solutions to fundamental societal challenges.	maximising the impact of EU-funded research.	routes aiming to turn R&I actions into concrete value and impact for society	
<b>Inform about and promote</b> the project AND its results/success.	<b>Describe and ensure results available</b> for others to <i>USE</i> > <b>focus on results only!</b>	<b>Make concrete use of research results</b> (not restricted to commercial use.)	<b>Focus</b>
Multiple audiences beyond the project's own community incl. media and the broad public.	Audiences that may take an interest in the potential USE of the results (e.g. scientific community, industrial partner, policymakers).	People/organisations including project partners themselves that make concrete use of the project results, as well as user groups outside the project.	<b>Target audience</b>

It is important to note that dissemination, communication and exploitation efforts may overlap. For this reason, this plan does not entirely separate all actions into the categories of 'communication', 'dissemination' and 'exploitation', as each action may serve all three aspects at any given time.

This document contains the communication and dissemination activities planned to address the M-Sec audiences (EU and Japan research communities, standardisation bodies, industry and SMEs, citizens, developers and smart cities stakeholders). It provides the tools to support all partners in promoting M-Sec, in engaging further stakeholders in the co-design of M-Sec solutions, and in disseminating the project results. The goal is to facilitate the analysis and adoption of the knowledge generated in M-Sec by the target communities, turning the solutions into socio-economically viable and sustainable innovations.

The Dissemination Plan is divided in the following sections:

- Target audiences
- Key messages
- Communication tools and channels
- Action Plan
- Monitoring and evaluation
- In a nutshell



## 2. Target audiences

The M-Sec target audiences were identified at the proposal stage. The following is a list of the main target groups that M-Sec is addressing and the strategies to reach each one. Possible cultural differences (Europe/Japan) will be considered.

**Table 2. M-Sec target audiences**

### General public (including Industry and SMEs)

**Who?** Public and private actors, such as city application developers, cities, organisations and SMEs, and national authorities.



**How can they benefit?** Understanding what the project is and its goals, considering how M-Sec could positively impact upon their day-to-day life in the cities of Fuijsawa and Santander, as well as in the future potentially being implemented in other locations.

**Which channels can we use to reach them?** Articles, press releases, newsletters, social media, videos, deliverables, website.

### Research community

**Who?** IoT, cloud, blockchain and big data researchers, not only from Europe and Japan but also on a wider international level, leveraging the strong industry-specific competences/expertise (e.g. cryptocurrencies in USA, nano-electronics in Asia).



**How can they benefit?** Adopting results, designing new collaborative research proposals, signing MoUs between research and industrial partners.

**Which channels can we use to reach them?** International conferences and workshops, publications in international journals, booths at exhibitions, newsletters, deliverables, website.

### Standards and Regulation bodies

**Who?** Main target groups are AIOTI - The Alliance for the Internet of Things Innovation, and OSGi alliance.



**How can they benefit?** Bringing the latest standards and regulations to M-Sec and, likewise, using the M-Sec project achievements for new standards and regulations.

**Which channels can we use to reach them?** Participation in European Commission consultations and other worldwide regulations in the field of interest, international conferences, international journals, deliverables.



### Cities field trial stakeholders / community (including citizens and startups)



**Who?** Potential end-users for each trial application, private or public players in the value chain, citizens' organisations with a bottom-up approach and citizens for public e-consultation.

**How can they benefit?** Learning about the technologies which may impact their day-to-day, engaging in the pilots and obtaining feedback during training activities. If beneficial, adopting the applications developed.

**Which channels can we use to reach them?** Co-organised training and community events (webinars, workshops, hackathons, etc.); online contests participated in by the startups and entrepreneurs; use cases replication in other cities; newsletters; social media; website.

### EU-Japan initiatives and policy makers



**Who?** Projects, initiatives and smart cities policy makers. Particular attention will be paid to creating clusters with projects already financed by the EU and NICT, under EU-JP calls.

**How can they benefit?** Developing synergies in order to cross-promote the activities and results, and to foster common accepted solutions in Europe and in Japan.

**Which channels can we use to reach them?** The EU's concertation activities; joint events; newsletters.

By targeting the audiences described above, M-Sec will strengthen the EU-Japan collaboration in the technological domains involving big data, blockchain, IoT and Cloud computing. Furthermore, it will facilitate the replication of M-Sec solutions in other smart cities.





### 3. Key messages

In order to convey a unified message about what M-Sec is about, the project team developed the following short description:

M-Sec is a collaborative project between the EU and Japan, strengthening connections in the technological spheres of Big Data, IoT, Blockchain and Cloud computing.

We empower social entrepreneurs, researchers, businesses, public authorities and citizens across the EU and Japan to work together, design and adopt new IoT applications, which improve the security and connectivity of smart cities, and facilitate trusted interactions between objects and people.

In addition, the following description was prepared for audiences with more technical knowledge:

M-Sec is a EU-Japan collaboration which stands for “Multi-layered Security technologies to ensure hyperconnected smart cities with Blockchain, Big Data, Cloud and IoT”.

The main goal of the M-Sec project is to research, develop, deploy and demonstrate multi-layered Security technologies to ensure hyper connected smart cities and empower IoT stakeholders with an innovative platform which leverages blockchain, BigData, Cloud and IoT security, upon which they can build innovative smart city applications.

The project explores secure, interoperable interactions between IoT elements based on a holistic secured cloud/edge/IoT context within a future smart city. Overall, the M-Sec paradigm complements mainstream IoT/cloud technologies, through enabling the introduction and implementation of specific classes of applications and services, which are not efficiently supported by state-of-the-art architectures.

M-Sec project will develop a diverse series of results for each WP. The key messages, elements and public deliverables to be disseminated per WP with support from WP5 are presented in the following table (all technical deliverables will be made public).

**Table 3. Key M-Sec elements and public deliverables to be disseminated**

Work Package	Key elements to be disseminated
<b>WP1</b>	<b>Project and Innovation Management</b> <ul style="list-style-type: none"><li>• M-Sec project objectives, activities and partners</li><li>• Consortium meetings</li><li>• Collaborations with the European Commission</li><li>• Submission of technical reports/project deliverables</li></ul>
WP1 Public	<ul style="list-style-type: none"><li>• D1.5 Data Management Plan (Month 6)</li></ul>



## Work Package

## Key elements to be disseminated

deliverables

<b>WP2</b>	<b>Use cases, Pilots and citizen involvement, integration and validation</b> <ul style="list-style-type: none"><li>• The M-Sec use cases</li><li>• The activities of the M-Sec pilots and how citizens will be engaged</li><li>• The development of the M-Sec platform</li></ul>
WP2 Public deliverables	<ul style="list-style-type: none"><li>• D2.1 M-Sec use cases description (Month 6)</li><li>• D2.2 M-Sec pilots definition, setup and citizen involvement plan (Month 8)</li><li>• D2.3 M-Sec pilots definition, setup and citizen involvement report – first version (Month 24)</li><li>• D2.4 M-Sec pilots definition, setup and citizen involvement report – second version (Month 36)</li><li>• D2.5 Integration Plan (Month 18)</li><li>• D2.6 M-Sec Integrated Prototype – first release (Month 21)</li><li>• D2.7 M-Sec Integrated Prototype – final release (Month 33)</li><li>• D2.8 M-Sec validation and overall evaluation (Month 36)</li></ul>
<b>WP3</b>	<b>Requirements, architecture, hyper connected smart city</b> <ul style="list-style-type: none"><li>• The M-Sec requirements analysis with potential end-users (corporate and citizens)</li><li>• The M-Sec architecture</li><li>• The risks and security elements of M-Sec in the context of a smart city</li></ul>
WP3 Public deliverables	<ul style="list-style-type: none"><li>• D3.1 M-Sec Requirements Analysis – first version (Month 8)</li><li>• D3.2 M-Sec Requirements Analysis – final version (Month 24)</li><li>• D3.3 M-Sec Architecture: Functional and technical specifications – first version (Month 12)</li><li>• D3.4 M-Sec Architecture: Functional and technical specifications – final version (Month 24)</li><li>• D3.5 Risks and security elements for a hyperconnected smart city (Month 24)</li></ul>
<b>WP4</b>	<b>Multi-layered security technologies</b> <ul style="list-style-type: none"><li>• The integration of IoT, cloud and data, blockchains and end-to-end security technologies in the M-Sec results</li></ul>
WP4 Public deliverables	<ul style="list-style-type: none"><li>• D4.1 M-Sec IoT security layer – first version (Month 18)</li><li>• D4.2 M-Sec IoT security layer – final version (Month 30)</li><li>• D4.3 M-Sec cloud and data level security – first version (Month 18)</li><li>• D4.4 M-Sec cloud and data level security – final version (Month 30)</li><li>• D4.5 P2P level security and M-Sec blockchains – first version (Month 18)</li><li>• D4.6 P2P level security and M-Sec blockchains – final version (Month 30)</li><li>• D4.7 M-Sec application level security – first version (Month 18)</li><li>• D4.8 M-Sec application level security – final version (Month 30)</li><li>• D4.9 M-Sec overall end-to-end security – first version (Month 18)</li><li>• D4.10 M-Sec overall end-to-end security – final version (Month 30)</li></ul>
<b>WP5</b>	<b>GDPR, dissemination, exploitation and sustainability</b> <ul style="list-style-type: none"><li>• M-Sec communication channels and materials</li></ul>



## Work Package

## Key elements to be disseminated

- Scientific publications
- Participation in conferences and events
- The M-Sec exploitation strategy
- The involvement of entrepreneurs and developers for experiencing the M-Sec results

### WP5 Public deliverables

- D5.1 Project's Web Site (Month 2)
- D5.2 Initial Dissemination Plan (Month 6)
- D5.3 Dissemination Activities Report - first year report (Month 12)
- D5.4 Dissemination Activities Report - second year report (Month 24)
- D5.5 Dissemination Activities Report - third year report (Month 36)
- D5.6 Market Analysis and Exploitation - first year report (Month 12)
- D5.7 Market Analysis and Exploitation - second year report (Month 24)
- D5.8 Market Analysis and Exploitation - third year report (Month 36)
- D5.9 Community Building Plan (Month 12)
- D5.10 M-Sec Online Contest event (Month 32)
- D5.11 M-Sec GDPR compliance assessment report (Month 24)



## 4. Communication tools and channels

### 4.1 Visual Identity

The branding for M-Sec has been strategised since the beginning of the project, with the development of an original and robust visual identity. All project communication materials will use the M-Sec logo and visual identity.

#### Project name

The project name “Multi-layered Security technologies to ensure hyperconnected smart cities with Blockchain, Big Data, Cloud and IoT” may be shortened to “**M-Sec**” or “**M-Sec project**” (never “MSec” or “M Sec” or M-sec). The project name should be used correctly at all times to ensure consistent project branding.

#### Logo and project colours

The project logo has been developed to visually represent the concepts of security, trust and stability:

- A shield shape enhances the feeling of safety (Figure 1);
- Coloured layers add a feeling of triple strength (Figure 1);
- Two matt blues and a muted red enhance a feeling of stability, courage and trust (Figure 2).



Figure 1. Shield shape added for security, and multiple layers were added for a feeling of triple strength



	RGB 238 114 96	WEB #EE7260	CMYK 0 67 58 0
	RGB 91 195 223	WEB #5BC3DF	CMYK 61 0 11 0
	RGB 0 61 88	WEB #003D58	CMYK 100 0 0 75
	RGB 0 0 0	WEB #000	CMYK 0 0 0 100

Figure 2. New M-Sec colour palette for trust and security



Figure 3. Example of M-Sec logos and visual identity

## Funding information

All communication materials and dissemination of results (for example, in promotional images, external press releases or articles, news/blog, print materials, etc.) should demonstrate visibility of EU and NICT funding, by displaying both the NICT and EU emblems, and including the following text:

“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).”

## Branded templates

The following templates have been created to facilitate internal communication and project activities:

1. Agenda;
2. Meeting Minutes;
3. Power Point;
4. Deliverables (and Word).

The M-Sec templates are available for all partners on Confluence, in WP5.

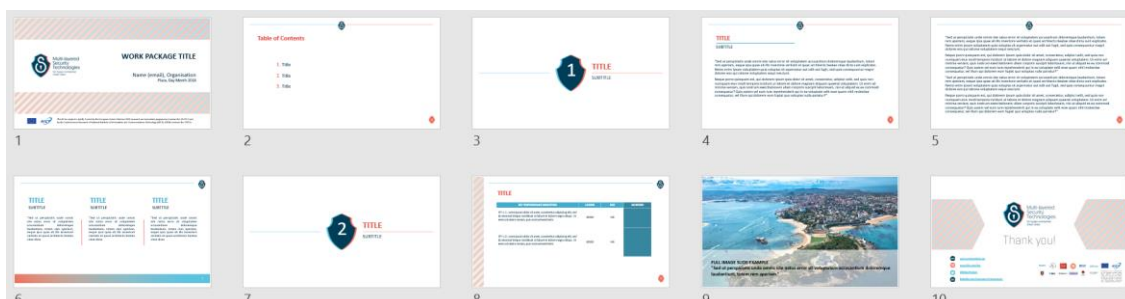


Figure 4. Example of M-Sec Power Point Template

**Action for partners:** Adopt the visual identity (logo, colours, funding information, templates) in all project communication and dissemination materials.



## 4.2 Project website

The M-Sec project website is available at [www.msecproject.eu](http://www.msecproject.eu). A dedicated deliverable regarding the project website (D5.1) has been submitted. The website promotes public awareness of the M-Sec activities and is available both in English and in Japanese. All public deliverables, scientific papers and communication documents will be made available on the website. The website will be maintained for 3 years after the project has ended to support the exploitation of the M-Sec results.

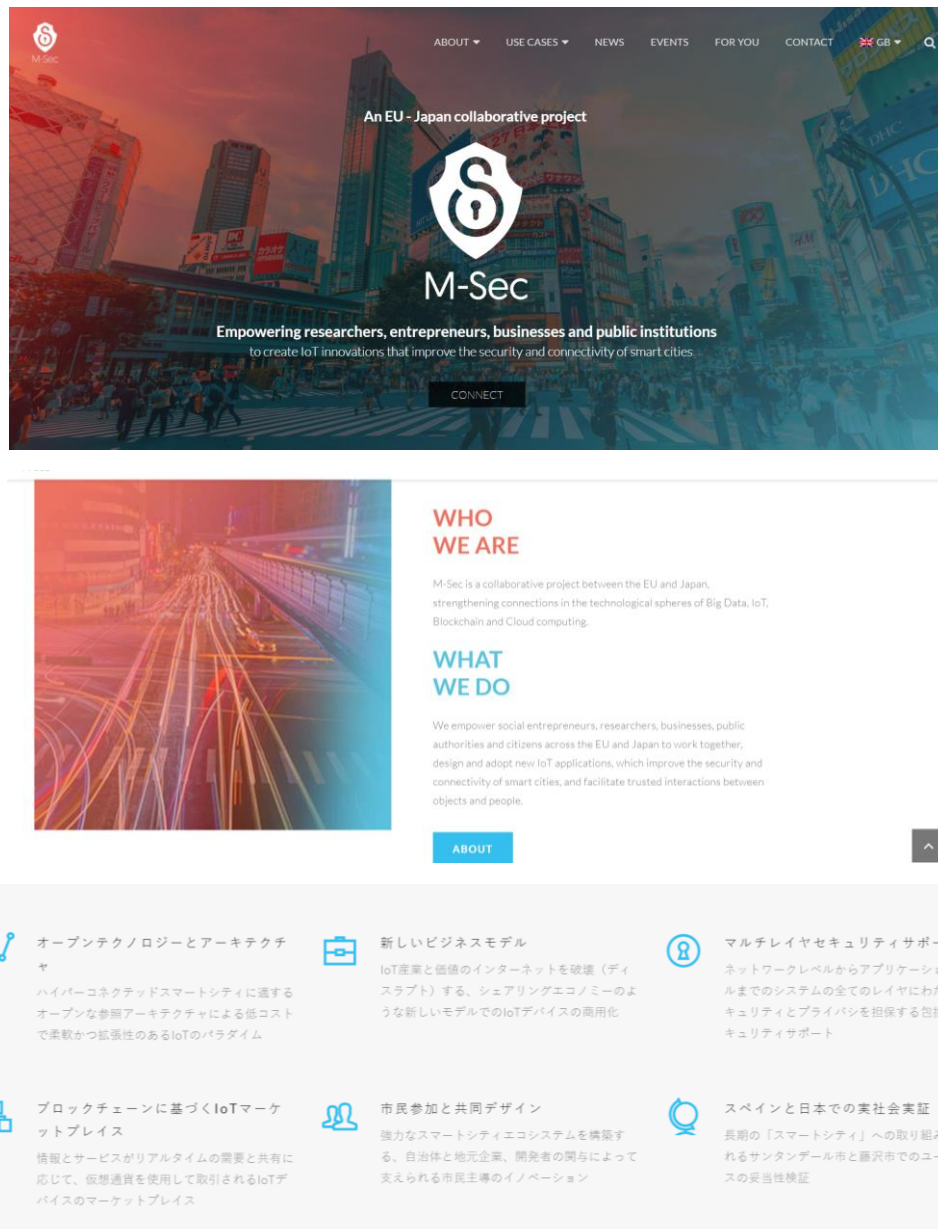


Figure 5. M-Sec project website - homepage screenshots (in English and Japanese)

**Action for partners:** Share information with F6S about events they are attending, any news they might have about the project for publication in the news section, as well as relevant scientific publications to be uploaded on the website. Request alterations on the website if necessary.





## 4.3 Social media

### M-Sec channels

M-Sec is present in the following social networks, to maximise the visibility of M-Sec activities and results, as well as the organisation and participation of international events:

- **Twitter:** [@MSecProject](https://twitter.com/MSecProject)
- **LinkedIn:** [M-Sec Project](https://www.linkedin.com/company/msec-project/)
- **F6S IoT:** [www.f6s.com/iot](http://www.f6s.com/iot) (community of IoT startups and SMEs)

These channels were chosen over other social media platforms such as Facebook, Instagram and Pinterest due to the more professional nature of their user bases, therefore increasing the probability of reaching the M-Sec target audiences.

F6S is responsible for keeping the social media accounts active and updating them with the project developments. All M-Sec partners contribute with content and news about their project activities, sharing these with F6S for publication.



Figure 6. M-Sec Twitter screenshot (November 2018)

### Organic social media strategy

- **Frequency:** Weekly activity, to be assessed in more detail as the project progresses
- **Time:** Early morning for Twitter (as a news platform), and afternoon for LinkedIn (professional platform).
- **Images:** It has been [reported](#) that tweets with images are 150% more likely to be re-tweeted and LinkedIn posts with images receive 200% more engagement than text-only posts.
- **Content:** M-Sec blog articles and project updates.
- **Use #MSecProject:** As well as well-established hashtags, such as #IoT or #blockchain
- **Use tags:** Tag in interested organisations or bodies.



## Partners' social media channels

In addition to the M-Sec social media accounts, the partners' social media channels (see 5.4 "Partners' channels") are also being leveraged for communication purposes, to make the most of their already established base of followers.

**Action for partners:** Read and follow the Social Media guide to guarantee successful communication of the M-Sec project via social media. The guide was developed by F6S and is available to all partners (Confluence WP5). Use the social media visuals that will be shared by F6S throughout the project.

## 4.4 News and articles

The following types of content will be developed to share M-Sec news with the target audiences:

- **M-Sec newsletter** – a project newsletter will be developed twice a year (6 in total). Visitors to the website can subscribe to the M-Sec newsletter.
- **M-Sec press releases** – press releases will be developed during relevant occasions of the project (estimation of 6), to be shared with local and international media. These press releases will follow a certain format, including a description of the project in general to raise awareness of the project, as well as the current news and information about the partners involved and funding.
- **M-Sec blog posts on the website** – the project website has a section for "NEWS", which is updated regularly with short articles about the M-Sec activities and developments.

The planning for the release of newsletters and press releases is presented on section 5 – Action Plan. The target audiences of this news includes research and innovation local and international media, as well as the initiatives and standardisation bodies that M-Sec aims to collaborate with – see section 4.8.

**Action for partners:** Share the newsletters, press releases and blog posts in their channels on a weekly basis (if applicable). Leverage existing press contacts and additional channels, sharing official M-Sec content. Contribute to the development of news by providing relevant information about their activities.



## 4.5 Promotional materials

A specific visual identity for promotion materials has been developed and is presented below. It includes a new image of a smart city, developed specifically for the project.

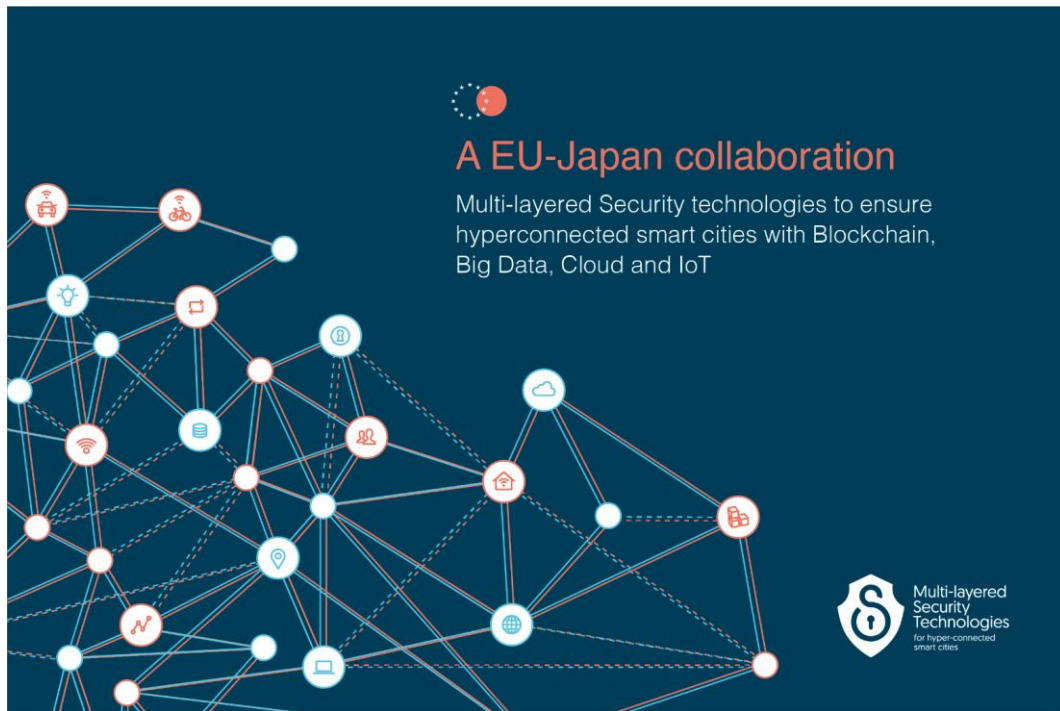


Figure 7. M-Sec Visual Identity for promotional materials



Figure 8. M-Sec smart city



The following promotion materials are planned, using the H2020 and NICT funding acknowledgements:

- **M-Sec Flyer / Postcard** – in A5 size, to handout during one-to-one meetings and events.
- **M-Sec Business Card** – in visiting card format, to handout during one-to-one meetings and events.
- **M-Sec Poster** – in A3 size, for display in the partners' facilities and events, as well as in M-Sec events.
- **M-Sec Roll Up** – to display in M-Sec events.
- **M-Sec Generic Power Point Presentation** – to adapt and use in presentations about M-Sec.
- **M-Sec Comics book** – for development at the end of the project.

The M-Sec Flyer / Postcard is presented below.



Figure 9. M-Sec Project Flyer/Postcard

**Action for partners:** Use the promotional materials during events/share by email. Inform F6S if more materials need to be developed.



## 4.6 Events

All partners will contribute to the dissemination of the M-Sec results by publishing papers on selected conferences, attending workshops and events, and presenting the results in relevant forum.

There are 2 types of events considered in the M-Sec dissemination strategy. Short videos may be developed presenting key moments, short testimonials or the recap of the events.

- **External events** – Participation in events for presenting the M-Sec results:
  - Presentation in international scientific conferences;
  - Demonstration in exhibitions.
- **Internal events** – Organisation of events for providing tangible experiences on the results:
  - Organisation of hackathon/ideathon/training workshops for developers and users;
  - Organisation of international research workshops (including in collaboration with similar projects and initiatives).

The following is a non-exclusive list of the planned participation in events during the first year of M-Sec.

**Table 4. Planned attendance to relevant events in the first 12 months**

Name of event	City, Country	Date	Partner(s) attending	Website
XVIII International Congress ORP conference	Cartagena de Indias, Colombia	18 September 2018	AYTOSAN	
IoT Solutions World Congress	Barcelona, Spain	16-18 October 2018	TST, Keio, Worldline	<a href="https://www.iotsworldcongress.com/">https://www.iotsworldcongress.com/</a>
Smart City Congress	Barcelona, Spain	November 2018	Worldline, AYTOSAN	<a href="http://www.smartcityexpo.com/en/home">http://www.smartcityexpo.com/en/home</a>
1st Smart Territories day	Santander, Spain	20 November 2018	AYTOSAN	
Symposium on ICT call (EU-JP collaboration)	Vienna, Austria	3 December 2018	Worldline	<a href="https://ec.europa.eu/digital-single-market/en/news/6th-eu-japan-symposium-ict-research-and-innovation">https://ec.europa.eu/digital-single-market/en/news/6th-eu-japan-symposium-ict-research-and-innovation</a>
ICT 2018	Vienna, Austria	4-6 December 2018	CEA, Worldline, F6S	<a href="https://ec.europa.eu/digital-single-market/en/events/ict-2018-imagine-digital-connect-europe">https://ec.europa.eu/digital-single-market/en/events/ict-2018-imagine-digital-connect-europe</a>
IEEE Percom 2019	Tokyo, Japan	11-15 March 2019	Keio	<a href="http://www.percom.org/">http://www.percom.org/</a>

**Action for partners:** Tag M-Sec on social media during the events. Fill in the events tracking file (see section 6.2) on a monthly basis.



## 4.7 Scientific publications

M-Sec partners plan a minimum of 15 scientific publications to be presented in international conferences with the results of the project, including 5 joint EU/JP publications. Three publications in international journals are planned as well.

The M-Sec scientific publications will be open access to comply with the general principle of H2020 and to boost knowledge and competitiveness on the M-Sec technologies in Europe and in Japan. This will be done by targeting publishers that provide “gold” access or using the “green” model when applicable.

**Action for partners:** Inform the M-Sec consortium when a scientific paper has been published (see section 6.2 – communication reporting).

## 4.8 Other channels

Over the duration of the project, the partners will come to know which sources are most interested in the M-Sec project and its results, facilitating the process with time. As such, further communication channels may be used for promoting M-Sec. Each partner will know the channels that it has access to and their relevance for the project communication and dissemination.

For instance, Santander City Council will communicate project outcomes through different municipal channels, including local newspapers, municipal buses, municipal buildings and through the organisation of meetings with local stakeholders. NTTE will promote initiatives to encourage local governments and other PR channels.

**Action for partners:** Adapt their individual communication strategy according to the most relevant channels for both the partner organisation and the local/international audiences. Use the communication budget wisely.

## 4.9 Synergies with other initiatives and standardisation efforts

### EU projects and smart city initiatives

M-Sec will establish synergies with other EU projects & smart cities initiatives. This may result in collaborations such as the co-organisation of events, the involvement of representatives of such initiatives in the M-Sec project (and vice versa), sharing knowledge and best practices, and the cross-promotion of activities and results, for an increased outreach of the project outcomes.

For communication purposes, an M-Sec communication kit will be shared with the responsible person of these initiatives to ensure the use of the M-Sec visual identity.









## Standardization bodies

In addition, M-Sec will identify opportunities to promote the M-Sec results and to influence standardization organisations and alliances, most of which the M-Sec partners are already active in. The upcoming table presents some of the standardisation organisations and alliances related to IoT, security, cloud, big data and blockchains, with which M-Sec aims to follow and/or establish a collaboration. The planned format of the collaborations is also presented.




**Action for partners:** Inform M-Sec partners of these synergies (read section 6.2 – communication reporting). Provide the necessary content for developing news articles about the collaborations.

**Table 5. Planned standardisation efforts**

Standardisation organisations and alliances		M-Sec partners involvement	
<b>AIOTI – WG 05</b> 	The Alliance for the Internet of Things, aims to give EU the lead in the Internet of Things (IoT) field creating a dynamic European IoT ecosystem	CEA	Contribute to working groups of smart cities, IoT Standardisation, IERC and smart living environment for ageing well
<b>IERC IoT (AIOTI WG 01)</b> 	IoT European Research Cluster – is bringing together EU-funded projects with the aim of defining a common vision of IoT technology	CEA, KEIO	Contribute to activity chains on - IoT Architecture and open platforms - Standardization for IoT Technologies - IoT Semantic Interoperability
<b>OSGi Alliance</b> 	Worldwide consortium of technology innovators that advances a proven and mature process to create open specifications that enable the modular assembly of software built with Java technology	CEA	Contribution to the IoT Expert Group with M-Sec requirements and technical results related to OSGi component architecture and services.
	FIWARE is a Private-Public Partnership (PPP) to develop the core technologies for the Future Internet and make those technologies available.	WLI (ATOS Group)	M-Sec platform will be FIWARE compatible and will be one of the contributors to the future FIWARE open source community
	Architecture and Protocol associated with M2M data transfer	KEIO	Contributing M-Sec results on Big city data generation, collection and redistribution
	Web of Things Working group focused on Web technologies for the IoT, in particular Semantic modeling, things metadata complementing existing semantics	ICCS	Contributing M-Sec results to the WoT community; enhancing IoT content with semantic metadata for allowing things to interact
	Elastic software deployments, interoperability	ICCS	Enable elastic deployments both horizontally and vertically for different layers of the M-Sec platform
	Application topology modeling, portable deployment	ICCS	Enhance the topology modeling of an application so as to allow portable deployment either to a centralized cloud





			infrastructure, or to the fog or the edge
<b>ITU-T GSI</b> 	IoT Global Standards IniSmart objects experience description and sharing exploiting extended social media technologies	ICCS	Contribution regarding the smart Objects that interact incorporating social media techniques for common experience sharing
 <b>IEEE</b> <b>P2413</b>	Standard for an architectural framework for the Internet of Things	NII	IEEE P2413 project will provide an architectural framework for the IoT and its sub-domains. NII will refer the architectural framework to design M-Sec architecture.
 <b>HYPERLEDGER</b>	Hyperledger project, Linux Foundation ( <a href="http://www.hyperledger.org">www.hyperledger.org</a> )	ICCS	Smart contracts, scalability issues of blockchains, Use Cases standardization, Requirements Working Groups



## 5. Action Plan

This Action Plan presents the main actions to be implemented throughout the project's lifetime. Most activities and materials to be developed have been planned at proposal stage.

### 5.1 Partner responsibilities

All partners will support the communication and dissemination of the project. The following table presents the responsibilities of all partners within WP5. WP Leaders have an increased responsibility of reporting on the activities of their WP.

Type	Activities
<b>Online communication</b>	<ol style="list-style-type: none"><li>1. Develop content for the project website (when requested + when an important activity will take/has taken place), and provide content in Japanese (when applicable)</li><li>2. Share content for the M-Sec social networks and interact with these accounts (following the instructions in the social media guide)</li><li>3. Include a section about M-Sec in their website, directing visitors to the M-Sec website</li><li>4. Contribute to the project newsletters (when requested) and disseminate these in their communication channels, as well as the project news</li><li>5. Publish articles in scientific journals and fill in the scientific papers tracking file – Confluence WP5</li></ol>
<b>Events</b>	<ol style="list-style-type: none"><li>6. Present the M-Sec project objectives and recent developments when possible (using the M-Sec Power Point template)</li><li>7. Inform F6S (WP5) of future participation in events – Confluence WP5</li><li>8. Distribute promotional materials to relevant stakeholders in meetings and events, or send PDF version by email (when applicable)</li><li>9. Display the M-Sec roll up during project events (when possible)</li><li>10. Collect records of participation in the events (photos, relevant resources) and fill in the events reporting file – Confluence WP5</li></ol>

Any contributions, suggestions or questions shall be addressed to F6S by email or on Confluence WP5. The tracking files are available on Confluence WP5.

Partners shall make use of their own communication channels and networks (website; social media; newsletters; cross-promotion through other projects; events – see upcoming section).



## 5.2 Communication timeline

The following table presents the main actions to be carried out during the entire duration of the project. The number of materials and timing of development are estimated, considering the key moments and potential needs of the project. The allocation of responsibilities among partners is also presented. The design of the materials is the responsibility of F6S and Santander City Council.

		Project Year 1												Project Year 2												Project Year 3											
		2018						2019						2020						2021																	
		J	A	S	O	N	D	J	F	M	A	M	J	J	A	S	O	N	D	J	F	M	A	M	J	J	A	S	O	N	D	J	F	M	A	M	J
Type	Main respons.	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36
Flyer	F6S/ATOS/NTTE																																				
Poster	F6S/ATOS/NTTE																																				
Roll up	F6S/ATOS/NTTE																																				
Generic Presentation	F6S/ATOS/NTTE																																				
Business Card	F6S/ATOS/NTTE																																				
Comics Book	F6S/ATOS/NTTE																																				
Press Releases	F6S/ATOS/NTTE																																				
Newsletters	F6S/ATOS/NTTE																																				
Toolkits/SDKs	ICCS/NII																																				
Scientific Papers	CEA/WU																																				
White Paper	TST/KEIO																																				
Tutorials/Cookbook	TST/KEIO																																				

Figure 10. Communication timeline



## 5.3 Partners' channels

The following table presents the channels which will be used by each partner.

**Table 6. Partners' communication channels**

		Website	Twitter	LinkedIn	Facebook	YouTube/other	Press releases	Newsletter	Blog/news
1	WLI	<a href="https://es.worldline.com/">https://es.worldline.com/</a>	<a href="https://twitter.com/WorldlineGlobal">https://twitter.com/WorldlineGlobal</a> <a href="https://twitter.com/WorldlineES">https://twitter.com/WorldlineES</a>	<a href="https://www.linkedin.com/company/worldlineglobal/">https://www.linkedin.com/company/worldlineglobal/</a>	<a href="https://www.facebook.com/WorldlineGlobal">https://www.facebook.com/WorldlineGlobal</a>		Yes	Yes	Yes
2	ICCS	<a href="http://www.iccs.gr/en/?noredirect=en_US">http://www.iccs.gr/en/?noredirect=en_US</a>							
3	CEA	<a href="http://www.leti-cea.fr/cea-tech/leti/Pages/Accueil.aspx">http://www.leti-cea.fr/cea-tech/leti/Pages/Accueil.aspx</a>	<a href="https://twitter.com/cealeti">https://twitter.com/cealeti</a>	<a href="https://www.linkedin.com/company/leti/?originalSubdomain=fr">https://www.linkedin.com/company/leti/?originalSubdomain=fr</a>		<a href="https://www.youtube.com/user/CEALeti">https://www.youtube.com/user/CEALeti</a>			
4	F6S	<a href="http://www.f6s.com">http://www.f6s.com</a>	<a href="https://twitter.com/F6SGov">https://twitter.com/F6SGov</a>	<a href="https://www.linkedin.com/company/f6s/">https://www.linkedin.com/company/f6s/</a>	<a href="https://www.facebook.com/f6s-289957147688809/">https://www.facebook.com/f6s-289957147688809/</a>			Yes	
5	TST	<a href="http://www.tst-sistemas.es/en/">http://www.tst-sistemas.es/en/</a>	<a href="https://twitter.com/tstsistemas">https://twitter.com/tstsistemas</a>	<a href="https://www.linkedin.com/company/tst/?originalSubdomain=es">https://www.linkedin.com/company/tst/?originalSubdomain=es</a>		<a href="https://www.youtube.com/user/TSTwireless/">https://www.youtube.com/user/TSTwireless/</a>			Yes
6	AYTOSAN	<a href="http://santander.es/">http://santander.es/</a>				<a href="https://www.youtube.com/user/AytoSantanderTV">https://www.youtube.com/user/AytoSantanderTV</a>			Yes
						Section on the website for EU projects			





7	NTTE	<a href="https://www.ntt-east.co.jp/en/?link_eastid=ins_h004">https://www.ntt-east.co.jp/en/?link_eastid=ins_h004</a>	<a href="https://twitter.com/NTTeastofficial/?link_eastid=ext_n002">https://twitter.com/NTTeastofficial/?link_eastid=ext_n002</a>	<a href="https://www.facebook.com/NTTeast/?link_eastid=ext_n001">https://www.facebook.com/NTTeast/?link_eastid=ext_n001</a>	<a href="https://www.youtube.com/channel/UCHIxUxTcZiuzHkBs9TGMptQ/?link_eastid=ext_n004">https://www.youtube.com/channel/UCHIxUxTcZiuzHkBs9TGMptQ/?link_eastid=ext_n004</a>	Yes	Yes
8	KEIO	<a href="https://www.ht.sfc.keio.ac.jp/">https://www.ht.sfc.keio.ac.jp/</a>	<a href="https://twitter.com/keiosfc">https://twitter.com/keiosfc</a>	<a href="https://www.facebook.com/keiosfc/">https://www.facebook.com/keiosfc/</a>		Yes	Yes
9	YNU	<a href="http://www.ynu.ac.jp/english/">http://www.ynu.ac.jp/english/</a>		<a href="https://www.facebook.com/U.YokohamaNational/">https://www.facebook.com/U.YokohamaNational/</a>			
10	NII	<a href="http://www.nii.ac.jp/en/">http://www.nii.ac.jp/en/</a>	<a href="https://twitter.com/jouhouken">https://twitter.com/jouhouken</a>	<a href="https://www.facebook.com/jouhouken/">https://www.facebook.com/jouhouken/</a>	<a href="https://www.youtube.com/user/jyouhougaku">https://www.youtube.com/user/jyouhougaku</a>	Yes	Yes
11	WU	<a href="https://www.waseda.jp/top/en">https://www.waseda.jp/top/en</a>	<a href="https://twitter.com/waseda_univ">https://twitter.com/waseda_univ</a>	<a href="https://www.linkedin.com/school/%E6%97%A9%E7%A8%B2%E7%94%B0%E5%A4%A7%E5%AD%A6/">https://www.linkedin.com/school/%E6%97%A9%E7%A8%B2%E7%94%B0%E5%A4%A7%E5%AD%A6/</a>	<a href="https://www.facebook.com/WasedaU">https://www.facebook.com/WasedaU</a>	<a href="https://www.youtube.com/user/wasedaPR">https://www.youtube.com/user/wasedaPR</a>	Yes
12	NTTDMC	<a href="http://www.keieiken.co.jp/english/">http://www.keieiken.co.jp/english/</a>	<a href="https://twitter.com/NTTDIOMC">https://twitter.com/NTTDIOMC</a>	<a href="https://www.linkedin.com/company/ntt-data/">https://www.linkedin.com/company/ntt-data/</a>	<a href="https://www.facebook.com/NTTDIOMC">https://www.facebook.com/NTTDIOMC</a>		







## 6. Monitoring and evaluation

### 6.1 Communication KPIs

In order to monitor and evaluate the dissemination and communication activities, a series of indicators were defined at the proposal stage. The table below presents the minimum targets to be achieved at project end, with support from all partners.

The status of each indicator will be collected at the end of each year and F6S/NTTE will monitor the indicators closely throughout the project. When necessary, the communication strategy will be readjusted to ensure maximum outreach towards the M-Sec target audiences.

**Table 7. M-Sec dissemination and communication indicators**

Indicators for measuring the effectiveness of the approach	Min target (project end)
Non-scientific publications (articles, press releases, ...)	15
Newsletters	4 newsletters
Video views	3000
Followers in social networks	> 500
Number of deliverables downloaded	200
Booth in exhibition	2
Publications in international conferences	15 incl. 5 joint (EU/JP)
Publications in international journals	3
Co-organized international workshops	2
Standardization groups that project interact with	> 3
Participation in EU commission's consultation and other worldwide regulatory in the field of interest	4
Number of training and community events co-organized (webinars, workshops, hackathons, etc.)	10, with 20-50 participants
Online contest with participation of startups and entrepreneurs	>1 with more than 20 participants
Number of citizens for e-consultation	1000 EU / JP
Use case replication in 2 cities or more	2



Indicators for measuring the effectiveness of the approach	Min target (project end)
Participation to EU's concertation activities	> 4
Joint events with other EU-Japan projects	> 4
Invitations from governmental institution (embassy, etc.)	> 3

## 6.2 Communication reporting

It is mandatory to report on the dissemination and communication activities. Communication reporting procedures have been established by F6S on Confluence WP5 to:

- i) Measure the communication indicators presented above;
- ii) Help F6S communicate any relevant activities/events through the M-Sec channels;
- iii) Adjust the communication strategy (when needed); and
- iv) Facilitate the task of providing the dissemination report to the EC.

### Method of reporting for partners

All partners are requested to report their communication efforts by filling in the designated tables directly on Confluence WP5 "M-Sec Communication Reporting":

1. Communication activities reporting;
2. Events planning/reporting;
3. Synergies with other initiatives.



## 7. In a nutshell

### Project Logo:



**Website:** <https://www.msecproject.eu/>

**Twitter:** <https://twitter.com/msecproject>

**LinkedIn:** <https://www.linkedin.com/company/msecproject/>

**F6S IoT:** [www.f6s.com/iot](http://www.f6s.com/iot)

**Hashtag:** #MSecProject

**WP5 Leaders:** F6S (Europe) and NTTDMC (Japan)

**Internal communication:** Defined under WP1

**Communication and Dissemination tools and channels:** M-Sec visual identity; project website; social media; news and articles; promotional materials; events; scientific publications; synergies with other initiatives and standardisation efforts.

**All materials:** Uploaded and made available to partners on Confluence – under WP5.

### Project Description:

M-Sec is a EU-Japan collaboration which stands for “Multi-layered Security technologies to ensure hyperconnected smart cities with Blockchain, Big Data, Cloud and IoT”. The main goal of the M-Sec project is to research, develop, deploy and demonstrate multi-layered Security technologies to ensure hyper connected smart cities and empower IoT stakeholders with an innovative platform which leverages blockchain, BigData, Cloud and IoT security, upon which they can build innovative smart city applications.

More information on <https://www.msecproject.eu/about/>.

### Funding acknowledgments:



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).

