



SMESEC

Protecting Small and Medium-sized Enterprises digital technology through an innovative cyber-SECurity framework

D6.4 Annual report on exploitation, dissemination and standardization (Year 3)

Document Identification			
Status	Final version	Due Date	30/05/2020
Version	1.0	Submission Date	08/06/2020

Related WP	WP6	Document Reference	D6.4
Related Deliverable(s)		Dissemination Level (*)	PU
Lead Organization	EGM	Lead Author	Philippe COUSIN, EGM
Contributors	FHNW UU ATOS	Reviewers	Christos Tselios, CITRIX
			Francisco Hernandez, WoS

Keywords:
Dissemination, market analysis, cybersecurity, SMEs

This document is issued within the frame and for the purpose of the SMESEC project. This project has received funding from the European Union's Horizon2020 framework Programme H2020-DS-SC7-2016 under Grant Agreement No. 740787 and supported by Swiss State Secretariat for Education, Research and Innovation (SERI) under contract number 17.00067. The opinions expressed and arguments employed herein do not necessarily reflect the official views of the European Commission.

This document and its content are the property of the SMESEC Consortium. All rights relevant to this document are determined by the applicable laws. Access to this document does not grant any right or license on the document or its contents. This document or its contents are not to be used or treated in any manner inconsistent with the rights or interests of the SMESEC Consortium or the Partners detriment and are not to be disclosed externally without prior written consent from the SMESEC Partners.

Each SMESEC Partner may use this document in conformity with the SMESEC Consortium Grant Agreement provisions.

(*) Dissemination level.-**PU**: Public, fully open, e.g. web; **CO**: Confidential, restricted under conditions set out in Model Grant Agreement; **CI**: Classified, **Int** = Internal Working Document, information as referred to in Commission Decision 2001/844/EC.

Document Information

List of Contributors	
Name	Partner
Cousin Philippe, Giunta Nicolas	EGM
Fricker Samuel	FHNW
Yigit Ozkan Bilge, Spruit Marco	UU
Ruiz José Francisco, Miranda Garcia Alberto	ATOS
Christos Tselios	CITRIX
Francisco Hernandez	WORLDSENSING

Document History			
Version	Date	Change editors	Changes
0.1	23/04/2020	EGM	Table of contents
0.2	6/05/2020	UU	Contribution standardisation
0.3	12/05/2020	ATOS	Contribution exploitation
04-05	29/05/2020	UU	Update standardisation part
06	1/06/2020	FHNW	Contribution dissemination chapter
07	1/06/2020	ATOS	Update exploitation
0.9	2/06/2020	EGM	Finalisation for review
0.91	4/06/2020	EGM	Corrections after review
1.00	08/06/2020	ATOS	Quality check and submission to EC

Quality Control		
Role	Who (Partner short name)	Approval Date
Deliverable leader	Philippe COUSIN (EGM)	05/06/2020
Technical manager		
Quality manager	Rosana Valle (ATOS)	08/06/2020
Project Manager	Jose Francisco Ruiz (ATOS)	08/06/2020

Document name:	Annual report on exploitation, dissemination and standardization (Year 3)	Page:	2 of 110
Reference:	D6.4	Dissemination:	PU
		Version:	1.0
		Status:	FINAL

Table of Contents

Document Information	2
Table of Contents	3
List of Tables.....	5
List of Figures	6
List of Acronyms.....	7
Executive Summary	9
1 Introduction.....	10
1.1 Purpose of the document	10
1.2 Relation to other project work.....	10
1.3 Structure of the document	10
2 Exploitation Activities	11
2.1 Exploitation Strategy.....	11
2.1.1 Joint Exploitation Plan	12
2.1.2 Individual Exploitation.....	15
2.1.3 Exploitation next step after the project end.....	24
2.2 Business Plan.....	26
2.2.1 Summary	26
2.2.2 Market Monitoring	26
3 Project dissemination	2
3.1 Dissemination strategy	2
3.1.1 Global approach and phasing	2
3.1.2 Objectives.....	3
3.1.3 Targets.....	4
3.1.4 Dissemination Messages	5
3.2 SMESEC Dissemination Highlights.....	6
3.2.1 SMESEC Survey V2.0	6
3.2.2 Feedback about Suitability of SMESEC Approach from Public Administration.....	8
3.2.3 Quiz on Cybersecurity Best Practices for SMEs.....	10
3.2.4 SMESEC Book.....	11

Document name:	Annual report on exploitation, dissemination and standardization (Year 3)			Page:	3 of 110
Reference:	D6.4	Dissemination:	PU	Version:	1.0
				Status:	FINAL

3.2.5	Press Releases about the SMESEC Framework Release.....	12
3.3	News and Events	15
3.3.1	News.....	16
3.3.2	Events	16
3.4	KPIs and Impact of SMESEC Dissemination	27
3.4.1	Awareness	27
3.4.2	Interest	30
3.4.3	Desire.....	31
3.4.4	Action	31
3.4.5	Scientific Dissemination.....	31
4	Standardisation Activities	33
4.1	Collaboration with European Organisations and Standardisation Bodies.....	33
4.1.1	ENISA’s Cybersecurity Standardization Conference 2020.....	33
4.1.2	ETSI TC CYBER	33
4.1.3	CEN/CENELEC JTC 13	34
4.1.4	ETSI ISG-CIM	34
4.2	Research Agenda: Cybersecurity Standardisation for SMEs	34
4.3	Guideline: Cybersecurity Standardisation Essentials for European SMEs	36
4.4	Results of the SMESEC Survey - Standardisation Related Questions.....	39
5	Conclusions.....	45
6	References.....	46
7	Annexes.....	50
7.1	Annex I IPR Agreement	50
7.2	Annex II Exploitation agreement	56
7.3	Annex III SMESEC- Letter of intent.....	14

Document name:	Annual report on exploitation, dissemination and standardization (Year 3)	Page:	4 of 110
Reference:	D6.4	Dissemination:	PU
		Version:	1.0
		Status:	FINAL

List of Tables

<i>Table 1: Dissemination target groups</i>	5
<i>Table 2: Dissemination message</i>	6

Document name:	Annual report on exploitation, dissemination and standardization (Year 3)	Page:	5 of 110				
Reference:	D6.4	Dissemination:	PU	Version:	1.0	Status:	FINAL

List of Figures

Figure 1: Compensation scheme diagram	13
Figure 2: FireEye offered services	27
Figure 3: Comodo information dashboard	27
Figure 4: ESET platform benefits	28
Figure 5: ESET information Dashboard	29
Figure 6: Open call survey results on budget allocation	31
Figure 7: Public survey results on budget allocation	32
Figure 8: Open call and public survey price preferences	32
Figure 9: Open call answers to benefit perception	33
Figure 10: Public survey answers to benefit perception	1
Figure 11: Overview of SMESEC dissemination approach	2
Figure 12: Dissemination plan	3
Figure 13: Overview of SMESEC dissemination objectives	4
Figure 14: SMESEC business model (thick blue frames: priorities for dissemination).	4
Figure 15: photos on showing massive attendance at FIC2020	19
Figure 16: design of the "wall" on the common EU Cybersecurity projects	20
Figure 17: P.Cousin and H. Baqua from EGM at SMESEC booth, FI2020	20
Figure 18: Cybersecurity Standardisation for SMEs: The Stakeholders' Perspectives and a Research Agenda Paper	35
Figure 19: The research design of the paper "Cybersecurity Standardisation for SMEs "	35
Figure 20: The 19 formulated research questions to steer future research on Cybersecurity Standardisation for SMEs.	36
Figure 21: Security Controls Presented in the Guideline	38
Figure 22: Unified set of security controls for use by SMEs	39

Document name:	Annual report on exploitation, dissemination and standardization (Year 3)	Page:	6 of 110
Reference:	D6.4	Dissemination:	PU
		Version:	1.0
		Status:	FINAL

List of Acronyms

Abbreviation / acronym	Description
AI	Artificial Intelligence
AST	Application Security Testing
CAGR	Compound Annual Growth Rate
CASB	Cloud Access Security Brokers
CBOR	Concise Binary Object Representation
DAST	Dynamic Application Security Testing
DDoS	Distributed Denial-of-Service
DLTS	Datagram Transport Layer Security
EC	European Commission
EDR	Endpoint Detection and Response
EGRC	Enterprise Governance, Risk and Compliance
EI3PA	Experian's Independent 3rd Party Assessment
EPP	Endpoint Protection Platform
EU	European Union
FISMA	Federal Information Security Management Act
GDPR	General Data Protection Regulation
GLBA	Gramm-Leach-Bliley Act
GRC	Governance, Risk Management and Compliance
HIPAA	Health Insurance Portability and Accountability Act
HTTP	Hypertext Transfer Protocol
IAM	Identity and Access Management
IAST	Interactive Application Security Testing
ICO	Information Commissioner's Office
ICT	Information and Communication Technology
IDS	Intrusion Detection Systems
IoT	Internet of Things
IPS	Intrusion Prevention Systems

Document name:	Annual report on exploitation, dissemination and standardization (Year 3)	Page:	7 of 110
Reference:	D6.4	Dissemination:	PU
		Version:	1.0
		Status:	FINAL

Abbreviation / acronym	Description
ISO	International Organization for Standardization
IT	Information Technology
IPR	Intellectual Property Right
JVM	Java Virtual Machine
KPI	Key Performance Indicators
LoI	Letter of Intent
MoU	Memorandum of Understanding
NGO	Non-Governmental Organization
OSS	Open source software and their communities
PCI DSS	Payment Card Industry Data Security Standard
PEST	Political, Economic, Socio-cultural and Technological
RASP	Run-time Application Security Protection
R&I	Research and Innovation
SAST	Static Application Security Testing
SDO	Standards Developing Organization
SIEM	Security Information and Event Management
SME	Small or medium-sized enterprise
SOX	Sarbanes-Oxley Act
SQL	Search and Query Language
SSL	Secure Sockets Layer
SWG	Secure Web Gateway
UEBA	User Entity Behaviour Analytics
UK	United Kingdom
URL	Uniform Resource Locator
USD	United States Dollar
UTM	Unified Threat Management
VPN	Virtual Private Network
WAF	Web Application Firewall
WP	Work Package
XSS	Cross-Site Scripting

Document name:	Annual report on exploitation, dissemination and standardization (Year 3)	Page:	8 of 110
Reference:	D6.4	Dissemination:	PU
		Version:	1.0
		Status:	FINAL

Executive Summary

SMESEC intends to deliver a lightweight unified framework to ensure cybersecurity of SMEs, key players in the value-added creation in Europe. Privacy, security are determining factors for massive IT deployments of new connected solutions and to ensure the renewal of most industry sectors. Combining consortium member's solutions, benefiting from the experience of 4 use cases in Internet of Things, Smart cities, Smart grid, eVoting, SMESEC aims at offering to SMEs an advanced cost efficient solution, easily accessible without an extended security knowledge or a dedicated team while improving SMEs awareness in the field with a dedicated plan integrated in the dissemination actions.

In the 3rd year the SMESEC framework was up and running and this report presents the three complementary activities to support the promotion of the Framework namely exploitation, dissemination and standardisation.

We explore all business and legal conditions to exploit the framework with the partners and we checked the market interest and readiness to use full or part of the SMESEC framework.

We disseminate the value of the SMESEC at face2face event such as big International Cybersecurity Forum FIC2020, at key workshop and with on-line dissemination actions such as mass mailing and survey.

Finally we succeed to contribute to standardisation cooperating with key standardisation bodies such as CEN TC 13 and ETSI TC CYBER. SMESEC contributes with a guide for SMEs which is going to be an ETSI Technical report.

Document name:	Annual report on exploitation, dissemination and standardization (Year 3)	Page:	9 of 110				
Reference:	D6.4	Dissemination:	PU	Version:	1.0	Status:	FINAL

1 Introduction

1.1 Purpose of the document

This document presents the current results of the SMESEC project on the 3rd year existence in the areas of dissemination, exploitation and standardization. It gives an overview of the performed work from all consortium partners and provide a more accurate view of the project roadmap with an update of the initial plan presented in the previous deliverable D6.3 at M24.

The global strategy is maintained for the coming months but as the technical part progresses, SMESEC integrated in its approach feedbacks from reached SMEs or representatives, inputs from other work packages experience to enhance the project impacts.

1.2 Relation to other project work

This work is based on all WPs and especially on WP2 and WP3 bringing inputs for technical understanding and use cases definition, in the creation of the security awareness plan, presented in the deliverable D2.3 at M6.

1.3 Structure of the document

This document is structured in four major chapters

Chapter 2 presents the SMESEC Business plan and exploitation strategy

Chapter 3 presents the performed communication activities, developed tools for the period M24-M36

Chapter 4 presents the standardization strategy plan, and the activities for the period M24-M36

Document name:	Annual report on exploitation, dissemination and standardization (Year 3)			Page:	10 of 110		
Reference:	D6.4	Dissemination:	PU	Version:	1.0	Status:	FINAL

2 Exploitation Activities

In this section, we present the exploitation activities and the results of these activities during the third year of the project.

2.1 Exploitation Strategy

The final approach to the exploitation strategy includes the following main efforts carried out by the consortium during this project period Year 3. The main objective was to describe the final steps to the project sustainability and how to cooperate to effectively transfer to market the consortium developments and generate a significant impact in the SMEs ecosystem.

The main topics addressed in this report, as detailed below in the subsection, include:

1. Joint exploitation
 - IPR
 - Commercial agreement
 - New legal entity
 - Letter of intent
2. Individual exploitation
 - Individual exploitation plans (final update)
3. Exploitation success stories
 - Start-up creation

All these activities are a final version (e.g. individual exploitation plans are final version which includes the final approach of each partner to the own exploitation of the project results based on previous iteration shown in D6.2 [43] and D6.3 [44], the IPR agreement is on the signature phase by a legal representative of each partner and the commercial agreement template covers all angles for a potential commercial opportunity).

Document name:	Annual report on exploitation, dissemination and standardization (Year 3)	Page:	11 of 110				
Reference:	D6.4	Dissemination:	PU	Version:	1.0	Status:	FINAL

2.1.1 Joint Exploitation Plan

2.1.1.1 IPR

During the last project period Year 3, the consortium partners have been working on the validation of the IPR agreement of the SMESEC developments, initially drafted during earlier phase of the project.

The sole purpose of this agreement is to reflect the distribution of the Intellectual property rights by components. This distribution is represented by a % of ownership.

The discussion around that ownership distribution, during this final phase, includes the agreement between partners with co-ownership of developments.

This final version includes, at that respect, all the project components. This encompasses components with a sole developer partner but also a fine grain approach to the above-mentioned co-ownership (e.g. CYSEC coaches or framework tool components).

The document has been submitted to all partners for its signature by a legal representative of each organization.

Additionally, this IPR agreement has been also integrated in the final version of the commercial agreement in order to be used as part of the compensation scheme. This commercial agreement will be used as a flexible approach to cope the commercial opportunities that the consortium could receive after the project ends. SMESEC IPR agreement is attached in annex I.

2.1.1.2 New Legal Structure

Another important pillar in the discussion of the exploitation strategy conducted during this Year 3 period is the definition and discussion of the generation of legal structure.

The main option studied regarding the legal partnership structures were, as previously described in D6.3 [44]:

- **New Legal Entity (Start Up):** develop a new legal entity that will be in responsible of the commercial activities of the project.
- **Joint Venture:** a business agreement between two or more partners acting together and sharing resources in pursuit of a business or in relation to a specific project.
- **Supply Chain:** several partners that contribute to delivering a component of product or service.

At the moment of writing this deliverable there was not a commitment from the consortium perspective to adopt or create any new legal entity to jointly exploit by the consortium members the project results.

2.1.1.3 Commercial Agreement

As previously mentioned, there is no official commitment from partner to create a new legal structure to continue with the commercial activities of SMESEC once the project finish, therefore the consortium looked for alternative options to carry out the joint exploitation of the project results, if the opportunity appears.

Document name:	Annual report on exploitation, dissemination and standardization (Year 3)			Page:	12 of 110
Reference:	D6.4	Dissemination:	PU	Version:	1.0
				Status:	FINAL

During year 2 a template version of a commercial agreement was presented to the partners, as described in D6.3 [44] . This agreement gives the consortium a flexible element to cope with any potential commercial opportunity that could appear in the future for the exploitation of SMESEC framework.

The flexibility comes from the perspective that the agreement does not need to be signed by all partners, only the ones that would have the intention to participate in a common exploitation of the results (the range of partner to be involved in it goes from bilateral to multilateral agreements).

During this reporting period, year 3, a more mature version has been designed and presented to the consortium partners. This final version of the agreement includes, additionally to the initial roles and responsibilities of each of the signing parts and a drafted compensation scheme, the Liability, confidentiality termination and also general clauses and a detailed description of the IPR agreement.

The agreement also describes the compensation scheme that the participant will have depending on their involvement. The figure below summarises the compensation approach.

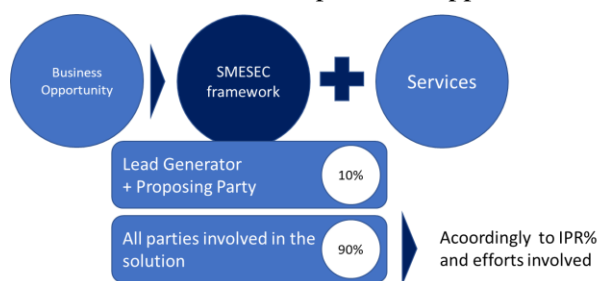


Figure 1: Compensation scheme diagram

The current version could be used as a template version for any potential commercial opportunity that the consortium could face. It is attached in this document as Annex II (7.2).

2.1.1.4 Letter of intent

In the subsection 2.1.1.2 of this document it has been mentioned that at the current moment there is non-official commitment, from the consortium partner perspective, to fund a new legal entity (i.e. start-up, new company or spin-off). Nevertheless, there is indeed an intention to extend the activities of the project after its lifespan.

At that respect a free willing commitment supported by SMESEC partners, in which each the consortium partners reflect their good faith to extend and continue their support to the project after its end, has been articulated in a letter of intent (LoI)

An specific template has been preped to accommodate each partner’s intentions. During the time this document is writing, several partners have detailed their intention to extend their support to the SMESEC activities (e.g. from training or consulting services to technical support or commercial activities).

The consortium considered this type of document rather than a Memorandum of Understanding (MoU) based on the assumption that the LoI can be a unilateral declaration (there is no need to reach an

Document name:	Annual report on exploitation, dissemination and standardization (Year 3)	Page:	13 of 110
Reference:	D6.4	Dissemination:	PU
		Version:	1.0
		Status:	FINAL

agreement among several or all partners, it can be just declared and signed by one partner). While a MoU is an agreement between several partners, and needs of the signature of all of them.

Among other activities, the partners intent to do:

- Provide all the assets, training material developed during the project’s life span under GPL licenses to all interested parties that will use SMESEC solution under contract.
- Provide installation guidance and support to the tools brought to the project
- Coordinate, any potential opportunity that may appear once the project ends.
- Maintained the SMESEC framework server running for a period of one year.
- Participate in the dissemination and communication of the SMESEC results and extend the dissemination activities with SMEs associations (e.g.Planetic).
- Proposing SMESEC solution along company’s product offering when technically and commercially relevant
- Maintaining the “Industrial Pilot” operative in Patras (Greece) and report on the functioning on the company’s website.
- Present the added-value of the SMESEC framework to selected customers and use reasonable efforts to attain an effective market adoption of the solution or some of its main components.

The LoI of all partners have been included as annexes in Annex III.

Document name:	Annual report on exploitation, dissemination and standardization (Year 3)			Page:	14 of 110
Reference:	D6.4	Dissemination:	PU	Version:	1.0
		Status:	FINAL		

2.1.2 Individual Exploitation

The present section provides the latest version of SMESEC partners' individual exploitation plans. This final version includes the last updates identified by each partner during Year 3. As a final version of a continues activity (the individual exploitation plan have been updated in each yearly report), some partner maintained their previous versions as no new opportunities have been identified:

Individual Exploitation Plan of Scytl	
PROFILE AND MOTIVATION	<p>1. Partner profile: Scytl is the worldwide leader in secure internet voting, election management and election modernization solutions. Its solutions incorporate unique cryptographic protocols that ensure maximum security, transparency and auditability in all types of elections. Scytl's groundbreaking electoral security technology is protected by international patents and it enables organizations to electronically carry out all types of electoral processes in a completely secure and auditable manner, positioning the company as the global leader in this industry.</p>
	<p>2. Your motivation to participate in the project and commitment: Within SMESEC, Scytl will be able to update its security solutions with more efficient mechanisms. The proposed real-life experimentations will evaluate the SMESEC framework for the e-voting use case. The identified most cost-effective cyber-security mechanisms will be integrated on the commercial offer of Scytl to provide more functionality and lines of protection for Scytl's clients.</p>
	<p>3. Means to achieve your objectives: Because of its expertise, Scytl is the internationally recognized leader in secure election management and electronic voting solutions. Over the last 10 years Scytl has electronically managed over 100,000 electoral events across more than 20 countries, including the USA, Mexico, France, Norway, Switzerland, Austria, BiH and India. Founded in 2001 as a spin-off from a university research group, Scytl has a strong commitment to R&D. Its current patent portfolio is the largest in the industry and is composed of more than 40 international patents in security applied to election processes.</p> <p>Scytl's solutions have been audited by independent organizations and by academic experts in the field of election administration that have consistently found its security and technology to be reliable and compliant with the highest security standards currently established. Scytl has capitalized on its 18 years of research experience to develop ground-breaking cryptographic protocols that secure the election registration, voting and results consolidation processes and are patent-protected. Scytl's technology and software are also protected by copyrights.</p>
	<p>4. Opportunity which appeared/appears: the main goal is to increase the security at the infrastructure level, as it currently is at application level only. Scytl will be able to offer its e-Voting service combined with a robust security framework that will allow SMEs and public authorities to implement high level security measures in their election processes without requiring a large budget. Such approach will help these entities to carry out secure consultation processes even with limited budgets.</p>
WHAT AND WHY	<p>5. Exploitable assets and results: Cost-effective cyber security mechanisms and training opportunities for SMEs. SMESEC will provide the security layer for hardening, monitoring, attack detection and prevention as well as a method to ensure the availability of the election process. The integration of both technologies will</p>

Document name:	Annual report on exploitation, dissemination and standardization (Year 3)	Page:	15 of 110
Reference:	D6.4	Dissemination:	PU
		Version:	1.0
		Status:	FINAL

	<p>provide a joint solution that will allow entities with limited budget to implement secure online voting processes with the highest levels of security, availability and transparency. Moreover, SMESEC will address the requirement for last minute code and service modifications to meet the peculiarities of each specific voting process.</p>
	<p>6. Your Value Proposition towards Joint Exploitation: the delivery of the framework that can be integrated in the system based on our customers’ needs. A use case will be provided by Scytl for testing purposes. The goal is to help local authorities and small public entities to improve and maintain the security controls of their ICT infrastructures with particular interest on last minute code and service modifications to meet the peculiarities of specific requirements.</p>
ROADMAP WITH TIMELINE	<p>7. Roadmap: During the first year of go-to-market, the bundled offering SMESEC/Scytl will be offered in France, Spain, US, Canada, Brazil and Australia to Governments bodies at national, regional and local levels as well as to other public entities, universities, associations, political parties and trade/labour unions.</p> <ul style="list-style-type: none"> a. SMESEC will be offered as a bundle to our current online voting offering and will not be sold as a standalone product. This bundled offering will be sold either directly through our sales force or through resellers/partnership agreements. b. From a promotional perspective, a landing page will be launched to promote the toolkit as well as all the related promotional materials, including brochure and powerpoint presentation. Promotional campaigns will be planned, including media, social media and emailing.
	<p>8. Measurement: As the SMESEC toolkit will be offered as a bundle to our current online voting offering, success will be measured mainly through metrics related to promotional activities. These metrics should include:</p> <ul style="list-style-type: none"> a. Volume and evolution of visits to the landing page or microsite that will be created to promote the SMESEC toolkit b. Reach of the media campaigns c. Volume of impressions and engagement rate related to the social media campaigns that will be launched d. Open and click ratio of the emailing campaigns that will be sent.
	<p>9. Positioning: Governments and private sector entities are showing increasing concern about cyber-security threats, particularly when it comes to introducing technology to electoral processes. On the other hand, they’ve had no other choice but embracing digital transformation over the past few years, and election processes is their next step. This is even more the case since the Coronavirus outbreak, which has caused elections to be postponed like in France, Spain or Italy. Therefore, as Governments and other entities adopt election technology progressively, it is important that their technology provider can ensure the highest levels of security to the new services they’ll provide.</p> <ul style="list-style-type: none"> a. By providing them with an additional security layer for hardening, monitoring, detecting and preventing attacks as well as ensuring the voting system’s availability throughout the election process, the integration of SMESEC into Scytl’s online voting offering will allow our customers and prospect to implement online voting processes with the highest levels of security, availability and transparency available to the market.

Document name:	Annual report on exploitation, dissemination and standardization (Year 3)	Page:	16 of 110
Reference:	D6.4	Dissemination:	PU
		Version:	1.0
		Status:	FINAL

	<p>b. SMESEC is aimed at bringing trust and confidence, not only to Scytl's online voting offering but also to the customer, who will be able to adopt technology with peace of mind.</p>
--	---

Individual Exploitation Plan of FORTH	
PROFILE AND MOTIVATION	<p>10. Partner profile: FORTH- Foundation for Research and Technology Hellas, one of the largest Research Institutes in Greece.</p>
	<p>11. Your motivation to participate in the project and commitment: We are willing to participated in any activities after the project's end as per the signed LoI and IPR agreements.</p>
	<p>12. Means to achieve your objectives: We can support SMESEC with bilateral contracts of technical support of the freely installed EWIS solution</p>
	<p>13. Opportunity which appeared/appears: Transfer of knowledge to the academic community. Enhance by integrating our solutions with Industry grade solutions that appear in the project.</p>
WHAT AND WHY	<p>14. Exploitable assets and results: EWIS platform as a whole or any of its individual components(LI Honeypot, SSH honeypot, IoT Honeypot, DDoS honeypot or cloud-ids)</p>
	<p>15. Your Value Proposition towards Joint Exploitation: Our system enhances other solutions active in the SMESEC like ATOS XL-SIEM and Citrix ADC, through the interconnection and exchange of security events and attack logs. Since our tools are built for research purposes and on top of Open Source tools and licensing schemes, we can provide all tools under the same open source licenses and provide an on-call support for the end-users of SMESEC.</p>
ROA DMA P	<p>16. Roadmap:</p>
	<p>17. Measurement:</p>
	<p>18. Positioning:</p>

Individual Exploitation Plan of BitDefender	
PROFILE AND MOTIVATION	<p>1. Partner profile: With over 1,600 employees, and a team of 800+ engineers and researchers, Bitdefender is one of the most innovative IT security software vendors in the world today. It works with government organizations, large enterprises, SMEs and private individuals across more than 150 countries. Dedicated to providing solutions to each of their challenges and needs.</p>
	<p>2. Your motivation to participate in the project and commitment: BD provides several security products that include anti-virus and anti-spyware capabilities against internet security threats such as viruses, Trojans, rootkits, rogues, aggressive adware, spam and others. Bitdefender applications include web protection, cloud anti-spam, firewall, vulnerability scanner, parental controls, document encryption and device antitheft as well as backup for corporate and home users.</p>

Document name:	Annual report on exploitation, dissemination and standardization(Year 3)	Page:	17 of 110
Reference:	D6.4	Dissemination:	PU
		Version:	1.0
		Status:	FINAL

R O A D M A P	<p>3. Means to achieve your objectives:</p> <p>Bitdefender will use SMESEC as a catapult to enter in the cyber-security market for SMEs and innovative digital solutions; the SMESEC use cases will be composed from innovative multi-technology solutions that will provide an incredible test board to evaluate the most interesting configuration about cyber-security for novel technology as IIoT, Smart City, etc.</p> <p>The main focus is on a more effective way to build on the existing SMEs and start-ups commercial approach, with the goal of consolidating and increasing the global market-share of SMEs niche.</p> <p>Also, more efforts were invested in communication activities to the existing Bitdefender client-base in order to:</p> <ul style="list-style-type: none"> a) inform as many clients as possible about SMESEC unified framework and its key-differentiators like complementarity of the integrated solutions, adaptability of its components, and affordability; b) raise awareness about the key-importance of deploying effective and complementary cybersecurity tools for those economic actors (SMEs and start-ups) which usually tend to ignore the constant cybersecurity threats due to internal ignorance and lack of awareness and the scarcity of resources in terms of both human and financial; c) collect relevant information about the dynamic cybersecurity needs within the SMEs sector; d) invite targeted clients to try the SMESEC framework after the project implementation. <p>Although the operations of the last months were altered by the pandemic wave of COVID-19, the constant efforts of BD teams pushed the information about SMESEC framework at various cybersecurity events (for both informative and commercial purposes).</p>
	<p>4. Opportunity which appeared/appears:</p> <p>Bitdefender aims to approach innovative solutions market by exploiting its experience on internet security. This will allow to potentially increase their sales even at short-term. Another exploitation action was to analyse and test possible partnerships of Bitdefender GravityZone with other digital solutions for various verticals (fintech, medtech etc.) in order to create bundles.</p>
	<p>5. Exploitable assets and results: previously described in the exploitation fiches [43]</p> <p>GravityZone is a business security solution built from ground-up for virtualization and cloud to deliver security services to physical endpoints, mobile devices, virtual machines in private, public cloud and Exchange mail servers.</p> <p>GravityZone delivers multiple layers of security for endpoints and for Microsoft Exchange mail servers: antimalware with behavioral monitoring, zero day threat protection, application control and sandboxing, firewall, device control, content control, anti-phishing and antispam.</p>
	<p>6. Your Value Proposition towards Joint Exploitation:</p> <p>Built around the GravityZone suite for Small and Medium Businesses, this approach was also aligned with the SMESEC general exploitation plan. The already established sales channels with various representatives of the European and Romanian SMEs associations facilitate a more concrete exploitation strategy.</p>
	<p>7. Roadmap:</p>

Document name:	Annual report on exploitation, dissemination and standardization (Year 3)	Page:	18 of 110
Reference:	D6.4	Dissemination:	PU
		Version:	1.0
		Status:	FINAL

8. Measurement:
9. Positioning:

Individual Exploitation Plan of UoP	
PROFILE AND MOTIVATION	<p>1. Partner profile: UoP is the third largest university in Greece with each own campus in the outskirts of Patras city. The Network Architectures and Management (NAM) group (http://nam.ece.upatras.gr/) which represent the research aspect of the Greek cluster in this project acquired its expertise through collaborations with industry and a series of research national and European projects. It is currently comprised of 2 professors, 4 post-docs, 2 researchers-system developers and 7 PhD students. During the last ten years, the NAM group has been involved in many Security, Future Internet Research (FIRE) projects like Panlab-PIL, OpenLab, FORGE, CIPSEC, SMESEC, CONCORDIA and 5G projects like 5GinFIRE, 5G-VINNI and coordinated others like VITAL++ and STEER. The NAM group of UOP is currently deploying a complete 5G facility in Patras, is maintaining the http://sence.city service that engages citizens to report issues across their city and is also the community coordinator of TheThingsNetwork IoT infrastructure for Patras</p> <p>2. Your motivation to participate in the project and commitment: Before SMESEC project, sence.city was supposed to be provided in a “free - as it is” agreement. However, one of NAM group’s goal was to be able to offer the sence.city service as a market product. To achieve this, we must address its low security levels. SMESEC project is an excellent opportunity to guide the UOP team in the security assessment, planning and implementation that will allow sence.city to reach a more mature business level.</p> <p>3. Means to achieve your objectives: UoP NAM group is formed by 2 professors and more than a dozen skillful scientists, engineers and developers which have been working together for more than 10 years. The group has participated in numerous projects the past 15 years and has a stable source of funding which allowed us to build a private cloud infrastructure and support our large set of software solutions, services and scientific projects. Currently the group is participating in 5 (five) H2020 projects and at the same time supports and operates a) the sence.city platform and b) TheThingsNetwork community using its own resources and funds.</p>

Document name:	Annual report on exploitation, dissemination and standardization(Year 3)	Page:	19 of 110
Reference:	D6.4	Dissemination:	PU
		Version:	1.0
		Status:	FINAL

WHAT AND WHY	<p>4. Opportunity which appeared/appears:</p> <p>Sense.city’s primary service is to allow citizens directly report to their municipality problems about the city. However, since the launch of this service various more business opportunities have been identified. In particular, the management and monitoring of IoT devices deployed around a city-wide area is one of the next features that this platform will implement as well as services for individuals with disabilities. Within SMESEC project UoP has the opportunity to work closely with one of the leading IoT SMEs in Europe (WoS) and through this collaboration a first set of IoT devices have already been deployed in one of the city’s biggest stadiums. This collaboration is an excellent opportunity for UOP to increase their portfolio on smart cities’ solutions.</p> <p>Another business aspect that UOP is also examining is to provide sense.city as a service to a 3rd company (SME/Industry) to integrate it to its Smart City related applications, thus expanding its portfolio in social networks, public administrations, smart cities etc. The security is a crucial matter to be addressed before moving forward with such a business deal. It must be ensured that both systems (UoP – company) are protected against each other, do not introduce security vulnerabilities and their personnel is trained to address the security challenges of the integration. The SMESEC project can provide to UoP high quality tools and solutions but also proper user training in order to support such kinds of business opportunities. Finally, as an academic institute, UoP is interested in building new collaborations with various partners to increase its research skills and develop a competitive portfolio of services that will allow us to participate in more national and international research or business projects.</p>
	<p>5. Exploitable assets and results:</p> <p>Within the context of SMESEC, our goal is to make use of part of the SMESEC framework and its high-quality tools to protect not only the sense.city platform but the entire private cloud infrastructure.</p> <p>Furthermore, inside SMESEC, UOP was able to successfully increase the security levels of another one of its services, the securityaware.me training platform. Now UOP can use this platform to host security courses for students, public servants using the sense.city platform as well as anyone else interested in learning about cybersecurity. Also, UOP will further promote securityaware.me as a candidate hosting platform for security training courses in external companies and other research projects.</p> <p>Finally, as an educational institute UoP will be able to improve its educational purpose by providing state-of-the-art knowledge and offer more bachelor diploma thesis and PhD positions in smart cities and security research topics as well as access to the research results of SMESEC</p>
	<p>6. Your Value Proposition towards Joint Exploitation:</p> <p>University of Patras is aiming to use SMESEC results to secure its UOP services and cloud infrastructures (used to host UOP services and research activities). Increased security allows the team to further develop its sense.city platform, address all the critical security and privacy requirements of a smart city application and eventually increase their market share by attracting more clients. An adequate number of clients would also allow UOP launch a spin-off company for the sense.city service. Furthermore, inside SMESEC, UOP was able to successfully increase the security levels of another one of its services, the securityaware.me training platform. Now</p>

Document name:	Annual report on exploitation, dissemination and standardization (Year 3)	Page:	20 of 110
Reference:	D6.4	Dissemination:	PU
		Version:	1.0
		Status:	FINAL

	<p>UOP can use this platform to host security courses for students, public servants using the sense.city platform as well as anyone else interested in learning about cybersecurity. Also, UOP will further promote securityaware.me as a candidate hosting platform for security training courses in external companies and other research projects. Finally, as an educational institute UoP will be able to improve its educational purpose by providing state-of-the-art knowledge and offer more bachelor diploma thesis and PhD positions in smart cities and security research topics as well as access to the research results of SMESEC</p>
ROADMAP WITH TIMELINE	<p>7. Roadmap: Following the time plan of SMESEC the target is to have the security framework installed and operational by M24. Then the UoP will contact municipalities which are currently using sense.city and discuss for any new services that they want and could be supported with these new security improvements. Also, as part of the re-evaluation plans for creating a new company, a self-sustainable spin-off will depend on its current customers and costs structure and forecast. This can be viable within the next one or two years</p>
	<p>8. Measurement: The impact of SMESEC project in sense.city service will be measured in the number of attacks we can identify and block and the number of successful attacks that cause issues in the normal operation of the service. Ideally with a more robust system we would like to increase the reputation of the service and the team and attract new customers and users (more municipalities and citizens). From the business point of view a growth in the customer critical mass will derive in a faster transition to the creation of the new legal entity. Finally, as part of the educational offer the number of bachelor diplomas and PhD in smart cities and security research</p>
	<p>9. Positioning:</p>

Individual Exploitation Plan of Worldsensing	
PROFILE AND MOTIVATION	<p>1. Partner profile: Worldsensing is a very active SME in innovation activities. Its core expertise is in providing sensing and machine-to-machine technologies and services to specific industry verticals. It has two mains product portfolios: one being smart traffic solutions for smart cities; and the other being heavy-industry monitoring solutions.</p>
	<p>2. Your motivation to participate in the project and commitment: Taking into account Worldsensing clients and targets, such company will exploit the security framework capabilities and skills acquired in this project to push its core business. Their typical clients are city councils and companies' owner and manager of big infrastructures.</p>
	<p>3. Means to achieve your objectives: SMESEC development, validated during the pilot phase, provide and extra layer of cyberresilience to attacks. Protection (antivirus) and monitoring capabilities (SIEM) are the most plausible licenses to be acquired.</p>

Document name:	Annual report on exploitation, dissemination and standardization (Year 3)	Page:	21 of 110				
Reference:	D6.4	Dissemination:	PU	Version:	1.0	Status:	FINAL

WHAT AND WHY	<p>4. Opportunity which appeared/appears: SMESEC will provide to Worldensing a fundamental knowledge for increasing the quality of the provided services in this context. After SMESEC this SME will be able to provide “reliable” Internet of Things applications where security threats are analyzed and minimized.</p>
	<p>5. Exploitable assets and results: Worldensing has been one of the project pilots and has integrated several components of the SMESEC framework</p> <p>6. Your Value Proposition towards Joint Exploitation: Worldensing intents include: Maintaining of the “Industrial Pilot” operative in Patras (Greece) and report on the functioning on the company’s website. Present the added value of the SMESEC framework to selected customers and use reasonable efforts to attain an effective market adoption of the solution or some of its main components. Keeping direct contact with the rest of project partners to respond to their needs in case they need Worldensing’s direct support to exploit SMESEC outcomes.</p>
	<p>7. Roadmap: During year one after the project, SMESEC framework would be presented to selected customers within WoS commercial portfolio.</p> <p>8. Measurement: The enhancements in the company commercial offer will open the door to many more business cases and thus to novel opportunities for increasing the number of clients and products sales.</p> <p>9. Positioning: The company has launched the CMT suite (Connectivity Management Tool), which is a SaaS layer on top to aggregate and display data. Invoicing is done taking the number of connected nodes as a reference (monthly fee per node).</p>
ROADMAP WITH TIMELINE	

Individual Exploitation Plan of ATOS	
PROFILE AND MOTIVATION	<p>1. Partner profile: Atos is a global leader in digital transformation with 120,000 employees in 73 countries. European number one in cloud, cybersecurity and high-performance computing, the group provides end-to-end orchestrated hybrid cloud, big data, business applications and digital workplace solutions through its Digital Transformation Factory. It also provides transactional services through Worldline, the European leader in the payment industry</p>
	<p>2. Your motivation to participate in the project and commitment: The motivation of Atos in the project is to grow our portfolio by enhancing our XL-SIEM solution with detection, reaction and correlation capabilities focusing in the specific aspects of SMEs, which form more than 90% of companies of Europe.</p>
	<p>3. Means to achieve your objectives: Atos Research & Innovation (ARI), has a dedicated team for market transfer of the technology’s enhancement developed in the research projects, the Innovation Hub. As a business development area team that works focus on facilitating the research</p>

Document name:	Annual report on exploitation, dissemination and standardization (Year 3)	Page:	22 of 110
Reference:	D6.4	Dissemination:	PU
		Version:	1.0
		Status:	FINAL

	<p>results to Atos global portfolio. The innovation hub can include the XL-SIEM in a dedicated accelerator (shuttle) to extend the evolution of the project results. Also, the cybersecurity department experts involved in the project will continue enhancing the XL-SIEM functionalities achieved in this project</p>
	<p>4. Opportunity which appeared/appears: SMESEC developments in cyber security solution focus in the SMEs domain fits in the ATOS Identity, Security and Risk Management commercial portfolio of solutions. The SMEs approach of the project showed a potential interest of a niche of customers that otherwise could not afford, from a budget perspective, a SIEM service.</p>
WHAT AND WHY	<p>5. Exploitable assets and results: XL-SIEM: Our solution provides, among other characteristics, identification of new and complex attack patterns, high-level risk metrics and correlation rules, user and entity behavior analytics, support for big data analysis, TLS certification for communication between the agents and SIEM, anonymization and encryption of data, and generation of heartbeats to monitor the status of the agents SMESEC framework: a platform where the user information, and cybersecurity tools, services and components developed by different parties, are integrated and hosted. The framework hosts from the consortium partners component to 3rd parties (via API) developments</p>
WHAT AND WHY	<p>6. Your Value Proposition towards Joint Exploitation: Atos is particularly interested in the outcomes of the SMESEC project as it will bring the necessary improvements and further enhance the AHPS-SIEM offering. Currently the AHPS-SIEM is operated mostly by security engineers that monitor activities from a wide variety of devices and then raise alerts as needed. Atos will test in XL-SIEM the enhancements provided by the outcomes of SMESEC project, which later on will be introduced in the next-generation SIEM of the company. The networking generated during this project with SME’s associations will extend Atos customer portfolio and this may have additional impacts in other areas of the company (Consulting, software factory, etc.).</p>
ROADMAP WITH TIMELINE	<p>7. Roadmap: The management of the Cybersecurity area have been participating in internal meetings with Research and Innovation to identify their current customers’ needs and how SMESEC components could be integrated in their portfolio offering. The components will be presented to the innovation board for an internal assessment to identify the suitability to become part of the Atos commercial portfolio . Additionally to this, SMESEC framework would be presented to target members of the fellow SMEs organization where Atos participates as an active member.</p>
ROADMAP WITH TIMELINE	<p>8. Measurement: Number of commercial opportunities schedule with the company portfolio customers.</p>
ROADMAP WITH TIMELINE	<p>9. Positioning:</p>

Document name:	Annual report on exploitation, dissemination and standardization (Year 3)	Page:	23 of 110
Reference:	D6.4	Dissemination:	PU
Version:	1.0	Status:	FINAL

2.1.3 Exploitation next step after the project end

The results of the project have helped to trigger two tangible sustainability action lines linked to the creation of new start-ups.

Each initiative has its own schedule (one has been already launched while the other one is in the transition between seed and start-up phase of the business lifecycle) but the common element for both is the experience and the enhancement of the commercial offer acquired during SMESEC project.

2.1.3.1 Sense.city – smart city pilot (UoP)

Inside the context of SMESEC, University of Patras (UOP) was responsible for the smart city pilot. The pilot focused on securing the sense.city, a smart city platform developed for citizens that want to report to their municipality problems they may have in relation to their city infrastructures and operations.

One of the peculiarities of this pilot was the fact that, contrary to the rest of SMESEC pilots (IoT, eVoting, Smart Energy), sense.city was a free tool created by a University and not a market product offered by a company. Thus, the development team, which was mainly composed by research stuff and students, had mainly focused on the functionality and features and did not pay too much attention on other aspects like business and marketing plans, security aspects, compliance with local regulations etc.

With the release of sense.city’s first version and its adoption by the municipality of Patras, UOP team realized that their solution had the opportunity to become an actual market product. But to achieve such a goal the team had to start working more professionally and adopt more business-oriented habits and practices. Such practices included market analyses, business plans, competitors’ products evaluation as well as security enhancements, regulations compliance etc.

At the same time the SMESEC project was starting and sense.city was one of the pilots that would evaluate the proposed security tools and solutions. University of Patras viewed their participation in this project as an opportunity to address several security requirements of the sense.city platform and its infrastructure (UOP cloud facilities). The team wanted to use the SMESEC framework to ensure that their service is provided to municipalities without introducing significant risks to their systems or data.

Inside the project, UOP adopted various security tools to protect the sense.city service. However, apart from the technical tools, SMESEC heavily influenced the security awareness of the lab. People involved in the development of the platform, realized that it was not just security components that were missing. Several required processes and security practices were overlooked and were directly putting the platform at risk. Security partners from SMESEC consortium helped UOP identify their critical vulnerabilities and based on their recommendations sense.city started implementing security plans, organized patch management, backup plans etc.

With better security in place, UOP began the development of a new “more sensitive” feature based on which, people with special needs can register their location inside sense.city and public protection authorities can dynamically adjust their operational plans in case an emergency incident takes place nearby. This feature was a “game-changer” in the market for smart city applications, since it was not offered by other platforms with similar functionality like the sense.city. With this feature, sense.city attracted the interest of many Greek municipalities which in turn led to increased resource requirements and personnel costs.

Document name:	Annual report on exploitation, dissemination and standardization (Year 3)	Page:	24 of 110		
Reference:	D6.4	Dissemination:	PU	Version:	1.0
		Status:	FINAL		

To be able to support its new costs, the team decided, from the beginning of 2020, to start charging the sense.city service. Also, it begun re-evaluating its plans for creating a new company. With the help of SMESEC partners (ATOS and WoS), they created a business plan and a roadmap towards the launch of a self-sustainable spin-off. The business plan revealed that based on its current customers and costs, the company is not yet viable, but it can be within the next one or two years. For this reason, the team decide to postpone the creation of the company. We must note that all budget estimations used for the business plan were based under the assumption that sense.city’s income comes only from its customers. A possible collaboration with funding schemes (angel funds, VCs etc.) would probably allow the creation of a company much sooner.

2.1.3.2 Start-up Creation (FHNW)

FHNW was enabling the creation of a start-up with the CYSEC Cybersecurity Coach. The company, XControl wants to mature and use CYSEC for automating advice to SMEs and offer scalable consultancy to many SMEs.

XControl with PIC 897666810 was established in Switzerland in 2019 as a start-up company driven by the observations that cybersecurity attacks shifted from large companies to small and medium-sized companies (SMEs). XControl offers coaching and tools that SMEs that often lack to mitigate incidents and respond to cyberattacks. XControl has been spun off from SMESEC project where automated self-adaptive cybersecurity coaching of SMEs has been piloted.

Small and medium-sized enterprises (SMEs) have been targeted by cyberattacks because they are hardly protected. This is an immense market: 99% of the companies are SMEs. Most SMEs are unable to invest in cyber security like large companies. Accordingly, the budget is often not sufficient for the assessment, installing tools and employee training. Advising SMEs on cybersecurity therefore requires new approaches and business models.

The start-up XControl want to develop an approach based on the principles of Virtual Coaching (VC) and exploiting the CYSEC tool that was developed in the SMESEC project. With the VC, XControl wants to make SME advice for cybersecurity affordable. Recurring topics in basic security topics should be modelled as a pathway and integrated into the work of the employees. The VC analyses the SME and supports the achievement of security goals with recommendations and feedback.

XControl has already started to develop a customer base for cybersecurity advice and services. It offers a tailored suite of cybersecurity sensor and shield tools adapted to the needs of SMEs and gives seminars and training for security awareness and capability improvement. The customers will be used as a basis to drive the maturation of CYSEC and automate cybersecurity advice with a Lean Start-up based process.

Document name:	Annual report on exploitation, dissemination and standardization (Year 3)			Page:	25 of 110
Reference:	D6.4	Dissemination:	PU	Version:	1.0
				Status:	FINAL

2.2 Business Plan

2.2.1 Summary

During Year 3, the market monitoring has continued, and updates have been described in this report in the following domains:

Market monitoring

- Supply side. Competitors
- Demand side. Market needs
- Surveys to end users. (Stakeholder analysis).

Business models

- The first approach of the Business Model Canvas SMESEC framework and the project pilots was initiated in D6.3 and the final version was presented in with a description of the sustainability approach with special focus on financial and acceptance

2.2.2 Market Monitoring

The market has been continuously monitored during the project lifespan and updates have been included in the yearly reports. The main focus in this report has been done in the analysis of market players which provide some toolkits with a similar approach to SMESEC framework.

Supply

2.2.2.1 Supply Side: Competitors

SMESEC framework as a whole product, is the integration of several components with a wide coverage of different segments of the security market. Apart from the range of competitors identified in earlier stage of the project, such as all the individual competitors per component (described in the exploitation fiches of the project components in D6.2 [43]), SMESEC framework will also be involved in a direct competition with some third-party solutions with a longer experience in the market. Some of the main ones were described during year 3 in D6.3 report. In this document the information is extended to other potential platform competitors:



FireEye [49] is a consolidated player in the cybersecurity market with over 2 decades of experience and more than 1 million hours per year on the frontlines of cyberattacks. Fire Eye provides the whole range of cyberthreat protection, from assesment to training courses. And a summary of the company profile includes:

- Over 700 intelligence experts
- 32 languages and 23 countries
- Over 380 red team engagements per year and more than 60.000 hours

Document name:	Annual report on exploitation, dissemination and standardization (Year 3)			Page:	26 of 110
Reference:	D6.4	Dissemination:	PU	Version:	1.0
		Status:	FINAL		

- More than 800 incident response engagements per year
- Over 1 million unique malware samples per day
- Headquarters in the USA



Figure 2: FireEye offered services

The company provide and extense courses catalogue web based but also provided by instructors. Several of the raining materials have a financial impact has they are not free.



Comodo [50] provides a complete cloud-native framework to protect companies' endpoints. This tool can provide a wide range of cybersecurity tool to provide breach protection which includes:

- End point security
- Managed detection & response
- Network security

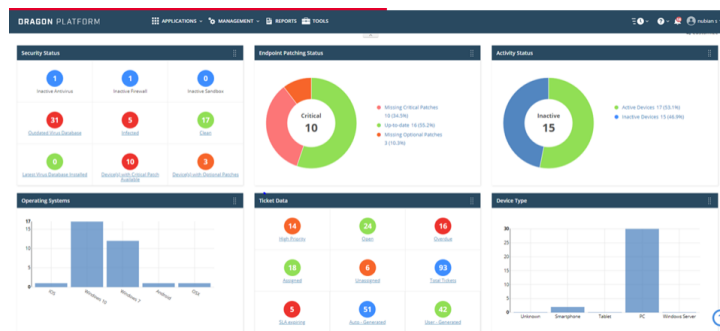


Figure 3: Comodo information dashboard

The summary of their market coverage is:

- 200.000 customers worldwide. They are in the market for some time now. Their customers goes from small to big companies
- 100million endpoints protected
- No training actives are offered but there is a possibility to have webinars on demand
- Offers a trial version

Document name:	Annual report on exploitation, dissemination and standardization (Year 3)	Page:	27 of 110
Reference:	D6.4	Dissemination:	PU
Version:	1.0	Status:	FINAL

- Headquarters in the USA



ESET [51] platform offers the level of protection that can be accommodated to a wide range of business. Each package includes individual standalone products for endpoint and server security, which have been bundled to make them more convenient for end customers.

Is a UK based company with headquarters in London.

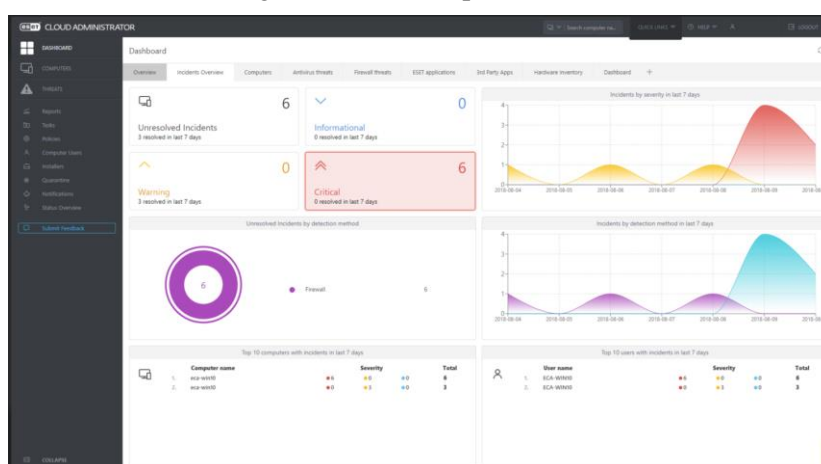


Figure 4: ESET platform benefits

ESET offer cloud-based services but also in-house deployment and also offers a trial version of each of the package solutions for a 30 days period.

The most popular package is the ESET Endpoint Protection Advanced Cloud (Cloud-based management) which provides:

Remote Management, Endpoint Security, Mobile Security, Virtualization Security, Server Security (although some services are not manageable via ESET platform at the moment.)



Document name:	Annual report on exploitation, dissemination and standardization (Year 3)	Page:	28 of 110
Reference:	D6.4	Dissemination:	PU
Version:	1.0	Status:	FINAL

Figure 5:ESET information Dashboard



Cyberalarm is a UK based company [52] which provides cybersecurity platform for SMEs to be launch during spring 2020 (you can register to receive information when it goes live)

- 24 hours a day vulnerability scan
- Email blacklists ad dark web. Also review of GDPR compromises
- Website, servers and hosting monitoring

A provider focus on SMEs. It uses a very plain language which tries to access “technology” reluctance companies.

Although has no training functionalities, they provide cybersecurity podcasts and articles related.

The majority of these solutions are already in the market, with a critical mass of customers and also, and particularly important in this sector, a reputational track. From a competition point of view, their offer covers some of the SMESEC framework components (endpoint protection) and also awareness and training are among their service catalogue.

At that respect and linking it with one of the main pillars of SMESEC project, the awareness creation and the training material can have a tangible impact in the SMEs ecosystem and is one of the strong points of the SMESEC framework to be remarked in its commercial offer.

2.2.2.2 Demand Side: Market needs

Cyber-attacks continued hitting during 2020 mayor companies around the world [47], but also hospitals or schools. Some of the latest examples of this attacks in 2020 include :

- Portuguese energy company Energias de Portugal (EDP) has been the victim of a RagnarLocker cyberattack. (10TB of sensitive data).
- Italian email provider confirms hack after users’ data found for sale on dark web (600,000 customers)
- Zoom accounts sold on the dark web (500,000 accounts)
- Online marketplace Quidd breached as users’ data goes on sale on the dark web (4 million users)
- Tesco issues customers new cards after credential-stuffing attack (600,000 customers)
- Boots says its Advantage Card database was hit by hackers (150,000 customers)
- T-Mobile notifies customers of cyber-attack on third party (impact unknown)
- Czech hospital bit by cyber-attack as it battles to contain COVID-19 (impact unknown)
- COVID-19 research facility 10x Genomics hit by ransomware (unknown)
- Wichita State University notifies students and staff of a security incident (1,762 students)

Document name:	Annual report on exploitation, dissemination and standardization(Year 3)			Page:	29 of 110
Reference:	D6.4	Dissemination:	PU	Version:	1.0
				Status:	FINAL

- Warwick University hid cyber-attack from affected staff and students (unknown)
- Cyber-attack on Indian property PropTiger exposes customers' data online (2,156,921 customers)

An accordingly to this continuous threat, the market forecast continue on the rise:

As part of the yearly market monitoring activities, the latest market forecast continue with the growing trend in the cybersecurity market. The global cybersecurity market is currently worth 173billion in 2020, growing to 270billion by 2026 [53]. . But also, a very relevant forecast is that by 2026, 77% of cybersecurity spending will be for externally managed security services [46]. This forecast shows SECaaS exploitation strategy as preferred option among the cybersecurity services providers, aligned with the business model approach of the consortium.

At this respect, The Manifest revealed that, at the time of the survey in December 2019, most small businesses (64%) said they were planning to allocate more resources to cybersecurity in 2020.

The current economic crisis due to the pandemic will have a negative impact in investment forecast. SMEs will redirect their financial efforts to the business survival and their operational activities.

Awareness and training are, specially in this situation, an extremely valid tool to leverage the importance of cybersecurity even in an extra limited budget situation as many SMEs can be facing at the moment.

2.2.2.3 Stakeholder Analysis

During year 2, and as part of the stakeholder analysis, the main stakeholder were identified and positioned in the Mendelow interest / power matrix, in D6.3 [44]. The main focus of the project was oriented to active stakeholders' group, mainly the SMEs. This group was identified as a key player in the transfer to the market of the project results, as they will be the adopters of the SMESEC developments.

After a first approach to European SMEs association (e.g. Praxis, ONTPE, PLANETIC or Schweizerischer KMU-Verbandin), the main activities related to this analysis during year 3 were focus on a deeper and direct engagement with some members of the SMEs ecosystem via an open call.

The main objective of the open call was the validation of the SMESEC solution with SMEs outside the SMESEC consortium. At that respect 4 different groups of SMEs were selected to conduct different activities during this open call (i.e. red team, integration via API, tools validation and feedback from a community of SMEs). All these activities are extensively described in D5.5 SMESEC Open call design, implementation and results report [55]

As part of this interaction with real end users, and their tangible experience with the project results, a survey was conducted to measure the real impact of the SMESEC framework in their organizations. Among these questions, an specific group of them was financially related and tried to understand the impacts for the participants from economic point of view.

Document name:	Annual report on exploitation, dissemination and standardization (Year 3)			Page:	30 of 110
Reference:	D6.4	Dissemination:	PU	Version:	1.0
		Status:	FINAL		

2.2.2.4 Survey open call

As part of the open call survey [55], some financial related questions were asked to the participants. These questions include, among others, their effort (budget related) to cybersecurity (i.e. What budget is allocated to cybersecurity?), and average price for the functionalities they consider key to enhance their cyber resilience (i.e. Which is the price, you as an SME, consider affordable?) but also how SMSEC could contribute to their organizations (i.e. Describe how do you think the SMESEC framework can contribute to your day-to-day business.)

In addition to this, a public survey was conducted via a questionnaire included in the project website. The results from both surveys are analysed in this section from an economic perspective.

The answers to these questions provided a good taste of the real SMEs' needs and how they can accommodate to the consortium assumptions related to:

- Pricing structure
- Customer needs

The results of these three main questions can be summarised as follows:

1. In terms of budget allocation (to cybersecurity), the answers provided reflect that almost a 70% of the companies have no budget allocated or they do not know. These results are aligned with the initial market analysis mentioned in the D6.1, only 27% of small businesses have a formally defined ICT security policy. Moreover, 29% of small businesses spend less than of 1,000\$ on IT security annually [54]

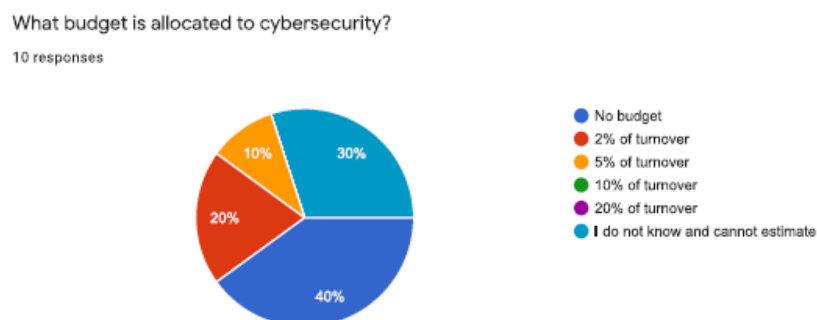


Figure 6: Open call survey results on budget allocation

Additionally to this, in the public survey of the SMESEC web the answers provided show a more active investment of the companies, but still a 55% of them have no budget allocated or they do not know.

Document name:	Annual report on exploitation, dissemination and standardization (Year 3)	Page:	31 of 110
Reference:	D6.4	Dissemination:	PU
		Version:	1.0
		Status:	FINAL

What budget is allocated to cybersecurity?

9 responses

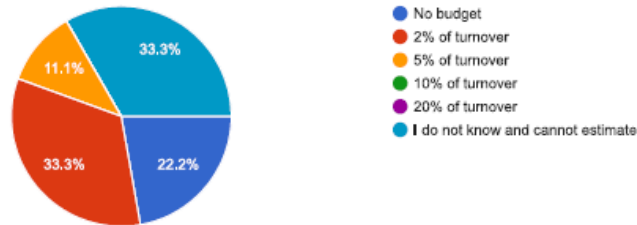


Figure 7: Public survey results on budget allocation

This lack of budget allocation and the subsequent cyberthreat exposure continue as one of the main tasks for the awareness creation.

2. Pricewise reflects a wider variety of answers The range of prices they consider affordable from their organizations ranges from 25€ head/month (in the lower part of the price range) to 85€ head/month (in the upper part of the price range).

Which is the price, you as an SME, consider affordable?

7 responses

Don't know

For our small company, 20.000 DKK

100 Euro/month

DKK 20000

10000 EUR

Not more than today

No idea

Which is the price, you as an SME, consider affordable?

10 responses

As a service: 2500-4000 €

180euro/year

<100 Eur per month (25 Eur per head)

\$100 per month

Don't know

question not applicable

30 euros/ month

1000-5000

3k

Figure 8: Open call and public survey price preferences

This information has been used as an additional input to benchmark the original approach of the consortium to its pricing structure. This price shows the intentions of the end users regarding the use of specific tools and not the whole SMESEC framework

This question aimed to gather information around one of the key pillars of SMESEC project, a budget friendly framework for SMEs.

Document name:	Annual report on exploitation, dissemination and standardization (Year 3)	Page:	32 of 110
Reference:	D6.4	Dissemination:	PU
Version:	1.0	Status:	FINAL

Although as described in D6.5 [48] in the pricing structure, the lower trench of SMESEC framework was on the limit of 7500€ (non-contemplated in the budget allocation of a high % of SMEs), this SMESEC basic package includes a wide range of tools that could exceed the SMEs coverage intentions. A tailor-made approach to each customer needs can accommodate both budget limitation vs the best cybersecurity approach to their organizations.

- On regards to how SMESEC could contribute to their organizations the main result of the surveys are linked to the awareness creation or acquiring knowledge. The participants express their main interest in increasing the cybersecurity awareness of their organizations. The technical offer is also taken into consideration as resilience and protection against cyberthreats is foreseen as a way to extend the viability of their organizations.

These answers reinforce the educational approach of the SMESEC framework as the door to open additional commercial opportunities.

Describe how do you think the SMESEC framework can contribute to your day-to-day business.

10 responses

1) Increasing my awareness 2) Protecting my SME 3) Being more resilient

Mostly on awareness since find it hard to integrate on cloud infrastructure

Global awareness about cybersecurity threats. Review of existing cyber solutions that might be used in a SME.

Mostly awareness and, less so, tools

Understanding and knowledge

it can not directly contribute, however the knowledge acquired is important to support the customers and to think about future business

properly identify cybersecurity-related risks for the organization (systems, assets, users, data, etc.), incorporate a tailor-made cybersecurity solution and discover cybersecurity events in real-time

By informing team members about cybersecurity status via one unified dashboard

With the growing numbers of employees and assets in our company, the ability of a unified management of security related issues would

Figure 9: Open call answers to benefit perception

Document name:	Annual report on exploitation, dissemination and standardization (Year 3)			Page:	33 of 110
Reference:	D6.4	Dissemination:	PU	Version:	1.0
				Status:	FINAL

Describe how do you think the SMESEC framework can contribute to your day-to-day business.

7 responses

News and critical information. Inspiration

I don't know

To be more safe when you are online

Overview and businesscase

Don't know

Knowledge to out it-team

No idea

Figure 10: Public survey answers to benefit perception

All the surveys were conducted prior to the COVID-19 and the results do not reflect the impact of the crisis in the real economy and specially in the SMEs ecosystem. In order to also address this new situation, a short interview was launched by mid-April 2020. These interviews try to see if the SMEs approach to cybersecurity has been impacted during a sudden event. At the time this document is written the number of answers is limited but they do not reflect yet a significant variation in their budget allocation intentions (i.e. SMEs still reflect a wide range of budgets to face their cybersecurity challenges and still the tranches vary from 200€/year, for a micro-companies, to 20.000€/year for a technological SMEs).

3 Project dissemination

The SMESEC scope implies, as a cybersecurity project, a wide range of actors, stakeholders that consortium will involve in its dissemination activities. Targeting all SMEs firstly, the project has reached a wide range of stakeholders such as SMEs organizations, sister H2020 projects, and local SME and cybersecurity specialists. The consortium continued dissemination according to the dissemination plan by focusing on informing the stakeholders about the piloting of the SMESEC framework, the release of the SMESEC framework, and the SMESEC project activities and outcomes.

The section here describes the project dissemination performed during M25-M36 according to the overall strategy, the dissemination initiatives, content and outcomes, and the dissemination monitoring for Year 3.

3.1 Dissemination strategy

3.1.1 Global approach and phasing

The experience-based project, the SMESEC framework has been developed upon the consistent feedbacks from use case SMEs from the IoT, Smart Cities, Smart grids and eVoting domains as defined in the DOA. This approach enabled the consortium to offer a SMESEC framework solution that meets the SMEs' needs and cost constraints. The SMESEC dissemination aimed at raising the awareness of threats and vulnerabilities of SMEs, raising interest for the SMESEC framework for these threats and vulnerabilities for SMEs, and making visible the significance of the knowledge about cybersecurity for SMEs generated in the project.

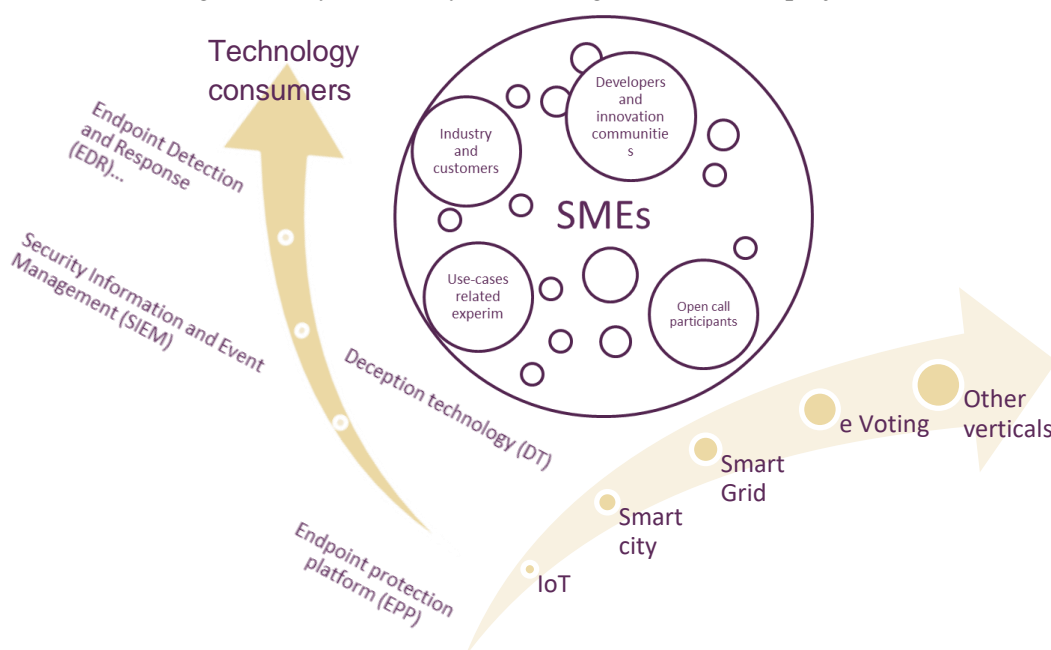


Figure 11: Overview of SMESEC dissemination approach

As presented in the figure above, the consortium developed a multi-channel plan to attract the widest audience addressing dedicated actions towards SMEs via direct interactions within the open call process, through SMEs organisation, offering a wide network of relevant project stakeholders. This main channel was strengthened by a set of verticals-based actions, taking advantage of the use case SMEs' experience to attract SMEs and a technology-based approach, focusing on security, privacy, and events and networks specialised in cybersecurity.

The figure below shows how all these activities were aligned with the SMESEC project plan. For the third year, the SMESEC dissemination aimed at informing about the piloting and release of the SMESEC framework. Also, SMESEC dissemination aimed at making visible the project work and the significance of the knowledge about cybersecurity for SMEs generated in the project.

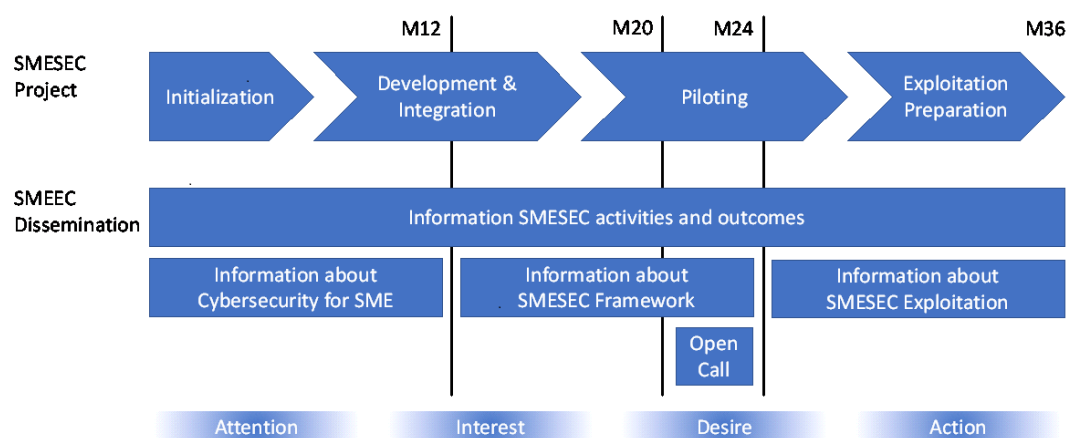


Figure 12: Dissemination plan

3.1.2 Objectives

The dissemination objectives are shown in the figure below. From a short-term point-of-view at the end of the project, dissemination firstly intends to ensure proper communication of all project outcomes and generate awareness and attractiveness of the SMESEC framework towards future users, in particular SMEs. These actions will support future standardisation and exploitation activities and trigger the adoption and implementation of SMESEC security framework while ensuring awareness of the wider SME and stakeholder audience.



Figure 13: Overview of SMESEC dissemination objectives

Further, the SMESEC consortium has decided to extend the SMESEC dissemination activities by co-authoring a jointly edited book that captures the wealth of knowledge of cybersecurity for SMEs that has been developed in the three years of project work. This effort has been made possible due to the limitations that Covid-19 has imposed on the participation in dissemination events in Spring 2020 with consequent postponement of scientific publications. The book is reinforcing the dissemination activities by making the results accessible to new audiences.

3.1.3 Targets

The dissemination performed by the SMESEC project during the third year was primarily intended to inform about piloting during the open call and release of the SMESEC framework according to the SMESEC business model. The figure below gives an overview of the SMESEC business model.










Key partners	Key activities	Value proposition	Customer relationship	Customer segmentations
 <ul style="list-style-type: none"> -Digital security experts -Big companies with expertise and contacts -SMEs providing use cases -3rd party HW/SW vendors 	 <ul style="list-style-type: none"> -Security modules integration and correlation -End-to-end real use cases in four European pilots -Training -Certification and standardization support 	 <p>Customer needs</p> <ul style="list-style-type: none"> -Protection -Simplicity -Cost-effective -Automation -Personalization -Training 	 <ul style="list-style-type: none"> -After sale services -Vulnerability assessment and continuous monitoring -Certification -360° feedback in specific tests 	 <ul style="list-style-type: none"> -SMEs offering solutions for the private sector and the public administration -Technology providers and service suppliers - Public administrations
	<p>Key resources</p>  <ul style="list-style-type: none"> -Security HW/SW solutions -SMEs code, products and services -Business experts 	<p>Products and services offered</p> Security framework and related services and modules	<p>Channels</p>  <ul style="list-style-type: none"> -Direct sales: meeting with CTOs -Trade fares, work-shop, seminars, etc. 	<p>Target costumers</p> -Service suppliers SMEs for the private sector (especially start up)
		<p>Open Call</p>		<p>Thought Leaders</p>
<p>Cost structure</p>  <ul style="list-style-type: none"> -HW/SW licences -HW/SW development -Trainings organization 		<p>Revenue streams</p>  <ul style="list-style-type: none"> -SMESEC framework licence -Staff training for certification -Services and value added consulting 		

Figure 14: SMESEC business model (thick blue frames: priorities for dissemination).

The table below shows the target audiences that the SMESEC dissemination was trying to reach. The target audiences were addressed with refined messages based on the market, and stakeholder segmentation described earlier in the deliverable D6.1. The primary focus of SMESEC dissemination were small and medium-sized enterprises. This target was prioritised over the other targets.

Target	Dimension	Segments	Information needs	Desired outcomes
SME	Size	Small	Goal-Oriented Hardening of a Digital Offering	Use and endorse SMESEC Framework
		Medium-sized	Goal-Oriented Cybersecurity in the Organization	
	Maturity	Start-up	Top-10 Hardening of a Digital Offering	
		Established	Sustaining Cybersecurity for whole Digital Portfolio	
	Domain	IoT	IoT-Specific Chapters	
		Smart Cities	Smart City-Specific Chapters	
		Other	Other Domains	
OSS	Product	Cybersecurity	How to bring OSS to SMEs	Integrate SMESEC Framework
		Other	Top-10 Hardening of a Digital Offering	Integrate SMESEC Framework
Academia	Discipline	Cybersecurity	Cybersecurity knowledge	Papers and citations
		Technology	Technology-oriented communities	
		Engineering	Security engineering for SMEs	
Policy	Region	EU, CH, Israel	Policy recommendations	Encourage SMESEC cybersecurity practice.
R&I	Region	EU, CH, Israel	Recommendations for economic development	Maturation and growth of SMESEC.
Individuals	Specialization	Opinion Leaders	Business-enablement with SMESEC.	Inform about SMESEC Framework
		Employees	SME protection and safety with SMESEC.	Use and endorse SMESEC Framework
		Public	Trust in protected SMEs.	Positive attitude towards SMESEC
SDO	Body	ETSI		Use SMESEC Results in Standards

Table 1: Dissemination target groups

3.1.4 Dissemination Messages

SMESEC started to implement the dissemination with a series of contents or stories that are kept consistent across channels. For year 3, they included: information about SMESEC piloting results, SMESEC framework release, and SMESEC project activities and outcomes.

The dissemination messages have been stable with just small modifications during year 3. The table below shows the message to be communicated by SMESEC dissemination.

Theme	Messages		
Importance of cybersecurity for SMEs	68% of SMEs experienced a breach or attack. 56% of breaches were not discovered within a suitable time. 60% of hacked SMEs closed within six months. Average cost of cybersecurity: 12'456€ for a small firm per year.		
Threats of importance for SMEs	<table border="1"> <tr> <td>DoS and DDoS Vulnerable Software Broken Authentication Misconfigurations Injection</td> <td>Cross-Site Scripting Sensitive Data Exposure Garbage Data Malicious Insiders</td> </tr> </table>	DoS and DDoS Vulnerable Software Broken Authentication Misconfigurations Injection	Cross-Site Scripting Sensitive Data Exposure Garbage Data Malicious Insiders
DoS and DDoS Vulnerable Software Broken Authentication Misconfigurations Injection	Cross-Site Scripting Sensitive Data Exposure Garbage Data Malicious Insiders		
Goals of Cybersecurity for SMEs	Cybersecurity must... ...be based on up-to-date facts and events ...activate and motivate all employees ...offer lightweight defences against cyber threats		
SMESEC Framework	SMESEC offers a lightweight cybersecurity framework for thorough protection, including... ...Awareness & Training Tutorials ...Vulnerability Discovery & Resolution Tools ...Definition & Recommendation Tools ...Threat Protection & Response Tools ...Lessons from Testing & Validation		
SMESEC Methodology	Framework Tested with Use Case and Open Call SMEs in... ...IoT ...Smart City ...Smart Grid ...e-Voting ...Digital Start-ups		
Advantages of SMESEC	Do it yourself: step-by-step guidance for meeting customer requirements and standards Keep the investment small: cost-effective tutorials and tools suitable for a busy environment Keep it simple: practices adapted to the company instead of complicated formal policies and procedures		

Table 2: Dissemination message

The core values that were pursued with the SMESEC messages and design of these messages were trust in SMESEC, respect of the expertise embedded in the SMESEC framework, and simplicity of the SMESEC framework. A professional designer packaged these values in the visual design used to communicate the SMESEC message to the target audience.

3.2 SMESEC Dissemination Highlights

3.2.1 SMESEC Survey V2.0

The original SMESEC survey was evolved to capture the knowledge gained during the first 2.5 years in the project, including the early results from the open call. The update to V2.0 was motivated by asking questions of even higher relevance for SMEs and offering guidance for the potential exploitation scenarios of the SMESEC framework.

We here present the answers that we have obtained for this second version of the survey.

Respondents

We have received 12 answers. 7 were micro companies with less than 10 employees, 3 were small companies with less than 50 employees, one was a medium-sized company, and one was a government agency or public organisation. 5 respondents were CEOs, 4 had a director position, 3 were consultants, and 1 was a developer.

The respondents were active in the following domains: 3 ICT, 2 professional services, 1 administration, 1 agriculture, 1 construction, 1 education, 1 manufacturing, 1 water supply, and 1 other. Within these domains, they pursued the following business models. Most common were development activities, and most common was the focus on software.

	Financial	Devices	Software	Data	Humans
Developer	1	3	6	4	4
Producer		3	3	3	3
Reseller		2		1	1
Service-Provider	1	1	2	3	3
Broker					

6 SMEs insourced software development (including the ICT companies), and 5 SMEs outsourced software development; only 1 the administration did both about equally. 6 SMEs hosted its software externally (including the ICT companies), 5 SMEs hosted some of its software internally and some externally, and the administration hosted all software internally.

10 of the 12 respondents were responsible for cybersecurity of their company, at least partly. However, only 4 had received any cybersecurity education. Accordingly, 8 SMEs had a dedicated person or team responsible for cybersecurity, 2 outsourced cybersecurity, and 2 had nobody responsible.

Exposure to Security Threats

7 of the 12 SMEs were worried about cyber threats. 4 SMEs considered themselves to be a target for hackers. In comparison to the previous year, 6 SMEs were more concerned, and 6 SMEs did not change their opinion.

The organisations depended on information that is available, kept confidential, and is integer. Only 1 organisation had low availability requirements, 1 other organization low confidentiality requirements, and 1 other organisation low integrity requirements.

Severe attacks that were a threat to operations were absent for all SMEs, however. Only 1 experienced occasional attacks that were moderate and required dedicated attention, and 7 experienced occasional or frequent attacks that were minor without significant impact.

The consequences of the attacks were as follows: 7 reported extra costs, 3 business disruption, 2 reputational damage, and 1 extra effort. 5 reported that most incidents had no consequences.

Role of Cybersecurity in the Respondent SMEs

The business of 7 of the SMEs would have difficulties with ICT outage of less than one day, 4 would still be operational if ICT would be off for more than one day.

0%-5% of the annual turnover was spent on cybersecurity: 4 had no budget, 4 spend 2%, 1 spends 5%. For 8 of the 12 SMEs, the spending on cybersecurity was about 50% of the SME's total ICT spending.

6 SMEs reported they have a systematic approach to cybersecurity, 4 reported they have not. 5 SMEs believed they can well mitigate cyber risks, 3 believed not. 6 SMEs believed they can easily recover from a cyber-attack, 2 believed not.

Cybersecurity Improvement

6 SMEs could consider pausing or slowing down their operations for improving cybersecurity, 3 could not.

The SMEs reported the following priorities for improving their cybersecurity (the table shows priority by number of SMEs):

Employee training	10
Extra budget	7
Advanced security solution	5
Security specialist	5
Improve tooling	4
Exchange with SMEs	4
Vulnerability search	3
Respond to priority threats	3

In average, the SMEs had the following preferences for sources of cybersecurity knowledge: external experts (Mean Opinion Score MOS 4.2), online courses and videos (MOS 3.8), webpages and online fora (MOS 3.7), and classroom courses (MOS 3.6). News were considered to be rather unattractive (MOS 2.5).

SMESEC Offering

10 SMEs considered SMESEC to be innovative, one considered it to be conservative.

No SME reported anything missing in the SMESEC framework. This indicates that they may not have the required expertise to judge the answer or could not spend the necessary effort in gap analysis of the SMESEC framework for their company.

The questions related to how to offer SMESEC have been answered inconsistently. The price suggestions varied by several orders of magnitude, the potential use of the framework was unclear, and no dominant distribution channel emerged. The heterogeneity of the answers is likely to be the result of the open-ended nature of the questions.

Security Standardisation

10 SMEs believed that information security standards improve the quality of their services and products. 4 of these positive respondents did not use any such standard, however. The other 6 positive ones used ISO/IEC 27001 (3x), the ones requested by their customers (1x), or others.

In average, the SMEs neither agreed or disagreed that there would be too many standards (Mean Opinion Score MOS 3.2), they slightly agreed that the standards were technically complex (MOS 3.7), agreed that the cost of standards acquisition is high (MOS 4.1), agreed that the cost of standards implementation is high (MOS 4.2), and neither agreed nor disagreed that the benefits of standards implementation was clear (MOS 3.2).

3.2.2 Feedback about Suitability of SMESEC Approach from Public Administration

The SMESEC approach has been evaluated by a representative of the **public administration of a political community with approximately 6500 inhabitants** located in Western Europe. The community has been chosen due to its size, which is twice the average size of the concerned country and the high level of technological maturity of the country. We expect that this critical choice sample represents an optimistic example of cybersecurity behaviour of a political

community. Smaller communities and communities in technologically less developed areas are likely to exhibit less awareness of cybersecurity and greater risk of incidents.

The feedback was received from a competent staff employee who was overseeing the community administration's ICT infrastructure, hence had relevant responsibility for the community's cybersecurity. The respondent did not have any specialized cybersecurity education.

Perception of Cybersecurity

The community did not see itself as a target for hackers; also, it did not aware of any cyberattacks on its ICT infrastructure in the past 12 months, not even minor ones.

The community is somewhat concerned of cyber threats; the concerns are unchanged in comparison to the previous year.

Exposure to Cyber Threats

The community manages personal data, sensible data, and intellectual property.

The following table shows the perceived criticality of cyber threats:

Level of Criticality	Treats
Critical	Virusses, compliance, privacy, user errors
Somewhat critical	-
Average criticality	System availability, malicious insiders, data integrity and availability, data loss or theft, spam
Little critical	Intrusion or manipulation of systems, system destruction or deletion, fraud, power outage
Not critical	Natural disasters

The community was not able to judge the following threats: system theft, integrity of transactions, ransomware and blackmailing, malicious outsiders, deception of users, and exposure of sensible data.

Management of Cybersecurity

The community believes that it can mitigate risks, vulnerabilities, and attacks to some extent but may have difficulties to recover from a cyberattack.

No systematic approach is institutionalized, however, to ensure the community's cybersecurity. For its defence, the community uses the following:

Category	Measures
Policy	Security baseline, guidelines for the use of computers, guidelines for the use of data
Physical	Physical access control, document shredder
Technical	Gateways and firewalls, VPN, regular updates, backup
Social	Employee training
Business	Insurances

The community considers online courses, webinars, and videos to be an attractive source for cybersecurity knowledge and expects external experts to deliver the that knowledge. Less attractive are physical courses or workshops, webpages and online for a, and newspaper, radio, or television. Out of scope is own research.

Cybersecurity is performed by a dedicated team, an external service provider. No dedicated budget has been allocated to cybersecurity.

Improvement of Cybersecurity

The community had no clear priorities for how cybersecurity should be improved. At the same time, it could not think of slowing and stopping its operations for improving its cybersecurity. If it would, it would train employees to strengthen the cybersecurity culture and contract cybersecurity specialists for improving the technical controls.

Potential for SMESEC

SMESEC has potential for increasing the community’s awareness of cybersecurity needs and for closing gaps in the cybersecurity of the community. The clearest gaps that could be addressed with SMESEC are described in the following table.

Category	Potential SMESEC Contributions
Policy	Transparency of attacks and incidents achieved with the SMESEC Hub, XL-SIEM, and the FORTH Honeypot. These tools could allow the community to understand how secure it is and set priorities for improving cybersecurity.
Physical	-
Technical	SMESEC could reinforce the community’s endpoint and network controls with the Bitdefender GravityZone and Citrix ADC, offering protection for system availability and against malicious insiders.
Social	SMESEC CYSEC could offer step-by-step guidance for capability improvement, allowing the community to set priorities for rapidly achieving all-over-the-board security, or for confirming that such protection has been achieved. Securityaware.me could fill gaps of online security training to the employees – the community’s preferred way of training.
Business	-
Other	IBM Anti-ROP and EGM TaaS have little relevance for the community, which is an ICT user and not an ICT developer.

3.2.3 Quiz on Cybersecurity Best Practices for SMEs.

SMESEC collaborated with the projects CyberWatching, CyberSec4Europe, and CyberWiser to mitigate the effects of the Covid-19 lockdown on the interest of potential end-user SMEs for SMESEC.

To attract interest for SMESEC online, as opposed to interacting with the public at a fair or conference, the consortium of cybersecurity projects offered a quiz on cybersecurity best practices for SMEs. SMESEC social media generated 76 conversions for this quiz.

Those who were successful and passed the quiz received a certificate as shown below.



3.2.4 SMESEC Book

In collaboration with the publisher Springer, a book was being prepared by the consortium to demonstrate the consortium’s knowledge about cybersecurity for SMEs and reinforce the relevance and validity of the SMESEC framework. The knowledge reported in the book was acquired during the technical project work and the many workshops of piloting the SMESEC framework and evaluating its impact in the SMESEC use case and open call SMEs.

The following shows the book outline:

<p>Title: Cybersecurity for Small and Medium-Sized Enterprises Sub-title: Resilience with Lightweight Tools and by Empowering Self-Reliance Editors: Samuel Fricker (FHNW), Christos Tselios (Citrix), Apostolos Fournaris (ATHENA), Jose Francisco Ruiz (ATOS) Publisher: Springer</p>
<p>Editorial: 1. Cybersecurity fo SMEs (FHNW, Citrix, ATHENA, ATOS)</p>
<p>Part I: Security Awareness and Knowledge 2. Threat Awareness and Risk Management (ATOS) 3. Cybersecurity Standardisation Essentials for European SMEs (UU) 4. Self-Reliant Capability Improvement (FHNW) 5. Educating a Cybersecurity Culture (UOP)</p>
<p>Part II: Technical Security Controls</p>

- | |
|---|
| 6. Endpoint Protection (Bitdefender)
7. Network Protection (CITRIX)
8. Honeypots for Attack Detection (FORTH)
9. Secure IoT Device Development (EGM) |
|---|

Part III: SME Case Studies

- | |
|--|
| 10. Protecting an IoT Business (WOS)
11. Cybersecurity for Startups (UOP)
12. Protecting a Software Services Company (GridPocket)
13. Hardening Electronic Voting (Scytl) |
|--|

At the end of the project in May 2020, 12 chapters were drafted and 10 chapters peer reviewed. The finalized book is expected to be submitted to Springer in June 2020.

3.2.5 Press Releases about the SMESEC Framework Release

To communicate the SMESEC framework release and the results achieved in the trial use of the SMESEC framework by use case and open call pilot SMEs, the partners ATOS (on behalf of the whole consortium), FHNW, and GridPocket authored a press release that they communicated to local media. While the key message of the framework release and successful piloting was shared by the three press releases, each partner added their own angle with a description of their own contribution and view of the project to their own press release.

The following shows the contents of the press release from ATOS:



The SMESEC consortium launches a framework to protect SMEs against cyber incidents

Madrid, May 27, 2020 – The SMESEC (Protecting Small and Medium-sized Enterprises digital technology through an innovative cyber-SECurity framework) **consortium, coordinated by Atos Spain**, released the first public version of the SMESEC Framework, a unified framework for Small and Medium-Sized Enterprises (SMEs). SMESEC helps SMEs to be protected against cyber-attacks and from the technical and awareness point of views. The project was a three-year multi-disciplinary innovation action co-funded by the European Commission and the Swiss State Secretariat for Education, Research and Innovation in the context of **Horizon 2020**, the EU Framework Programme for Research and Innovation. In comparison to other approaches, the SMESEC framework targets SMEs' specific needs and is priced with the SME's budget in mind.

Cybersecurity has become a critical problem for SMEs. According to the Verizon 2019 Data Breach Investigations Report, **43% of cyberattacks target small businesses**, as opposed to large companies. Among the most common problems are attacks of the SME's IT infrastructure with hacking and malware. At the same time, social attacks and errors or misuse of employees together also concern about half of the SMEs. According to the Cybercrime Magazine, **60% of small companies go out of business within six months after a critical cyber incident**.

The **SMESEC Framework** allows the end-user SME to self-assess its security status, secure its IT infrastructure, and develop a security-in-mind culture among its employees. The framework dashboard provides to its end-user SMEs, the ability to **understand its security level** and what the immediate steps are to become more secure. Christos Tranoris from sense.city (Greece): *"It was easy to retrieve and query for security events."* The **technical controls** included in the framework are intuitive and can easily be used by the SME for protecting computers, servers, and network and for detecting various incidents. Simon Gassmann from Quilvest (Switzerland): *"We could add a layer of security that protects us from attacks."*

The SMESEC Framework also encourages the end-user SME to appoint a Chief Information Security Officer (CISO), even as a part-time role. The framework offers **awareness** of cyberthreats, vulnerabilities, and risks to the CISO. Andreas Last from Grid Pocket (France): *"SMESEC gave us holistic awareness about cybersecurity."* It provides **step-by-step guidance** for installing controls. Olmo Rayon, from Worldsensing (Spain): *"The questions offered by SMESEC are so valuable for a CISO at the beginning of the career. SMESEC offers any company wanting to make its employees aware and have a clear overview of how to secure the company a structured way of assessing and planning."* It also provides **training for the employees** in defending the company against attacks and other incidents. Amalia Kakaroumpa from Myrtian Blue Events (Greece): *"I learned the basics of Spam and Phishing."*



The SMESEC Framework also includes **specialised tools for SMEs that offer digital products, services, and solutions**, allowing these SMEs to enhance their business with cybersecurity. Jordi Cucurull from Scytl (Spain): *“The SMESEC framework provided valuable insights into the security of our company and gave us, offering electronic voting solutions, security advantages that turned into business opportunities.”*

The SMESEC consortium **developed and piloted the SMESEC framework with twelve SMEs of diverse sizes, types, and industries**. Four of the SMEs are members of the consortium, and the others joined for trying SMESEC and evaluating its impact with an open call. The SMESEC framework and tools were installed and tested within these SMEs. Several workshops were conducted to understand the SMEs’ needs and impact of the SMESEC solution.

Jose Francisco Ruiz, the project coordinator, reflected on how this new cybersecurity approach could help SMEs in Europe: *“SMEs want to go digital, but they are worried about the cost and their exposure to hackers. With our solution, we want to help the SMEs to protect their business and their employees; both are equally important. Also, we discussed with SMEs their economic situation and found a realistic strategy.”*

Atos Spain, the coordinator of the project, thanks to its experience in the management of European research projects and business development, has taken part in the conception, production, integration and delivery of the SMESEC Framework. Moreover, Atos has also contributed in several technical activities – such as the management of requirements, system modules development, and testing and validation of the solution – to ensure the success of the final deployment in Europe. Finally, Atos has brought to SMESEC enhancements of its IEM tool, which provides event correlation for the detection of security incidents, integrating sensors from different solutions in the project, providing real-time alerts, and reporting and visualisation capabilities.

The project has brought a refined solution that has been tested with external companies and a red team to increase its resilience. Discussions with SMEs have shown that the SMESEC solution meets these SMEs’ needs and concerns and is considered very helpful for them. SMESEC doesn’t only allow the SMEs to use tools that fit their business well but also provides cybersecurity training and self-assessment for their employees. These capabilities, together with a tailor-made business strategy, make SMESEC attractive SMEs, which represent the majority of the European economy.

About SMESEC

SMESEC is a co-funded project of the European Commission and the Swiss State Secretariat for Education, Research and Innovation under the field of Information and Communication Technologies (ICT) of the H2020 Framework Program. The project started in June 2017 and is coordinated by Atos. It involves the following partners: Worldsensing (Spain), Panepistimio Patron (Greece), Foundation for Research and Technology Hellas (Greece), Easy Global Market



www.smesec.eu

(France), SCYTL Secure Electronic Voting (Spain), GridPocket (France), Fachhochschule Nordwestschweiz FHNW (Switzerland), Citrix (Greece), IBM Israel - Science and Technology (Israel), BitDefender (Romania), and Universiteit Utrecht (Netherlands).

More information about the project is available at www.smesec.eu

Contact

Jose Francisco Ruiz, ATOS Research & Innovation, josefrancisco.ruiz@atos.net, +34 91 214 8483

Follow us on Twitter [@SMESEC_EU](https://twitter.com/SMESEC_EU)

The press releases can be downloaded with the following links:

Partner	Press Release
ATOS	https://www.smesec.eu/doc/SMESEC_Press_Release_FINAL_ATOS_200527SFR.pdf
FHNW	https://www.smesec.eu/doc/SMESEC_Press_Release_FINAL_FHNW_200527SFR.pdf
GridPocket	https://www.smesec.eu/doc/SMESEC_Press_Release_FINAL_GridPocket_200527SFR.pdf

3.3 News and Events

The following information about news and events was published on the SMESEC homepage on www.smesec.eu.

3.3.1 News

SMESEC Standardisation Task's Outcomes presented to ETSI TC Cyber

May 19, 2020
Utrecht University

On May 19, Utrecht University presented the SMESEC project and the outcomes of the standardisation task to ETSI (European Telecommunications Standards Institute) TC CYBER. ETSI is one of the three standards developing organisations (SDOs) in Europe, and it has a technical committee (TC) for cybersecurity, TC CYBER.

As a follow-up to the [Cybersecurity Standardisation Conference 2020](#), Marco Spruiel (the leader of the standardisation task in the SMESEC project) invited in ETSI TC CYBER to present the SMESEC project and the outcomes of the standardisation task (T6.3) in particular in a TC CYBER meeting. The agenda of the presentation was as follows:

- * SMESEC introduction
- * Cybersecurity for SMEs: From standardisation stakeholders' workshop to research agenda
- * Cybersecurity standardization "where-to-start" guideline for European SMEs
- * Cybersecurity maturity assessment of /for SMEs
- * What's next?

The contributions of the standardisation task were well received. For the SMESEC, a follow-up collaboration has now been initiated specifically for the "Cybersecurity standardization "where-to-start" guideline for European SMEs." The CEN/CENELEC representative requested the same presentation in an upcoming CEN/CENELEC meeting. We appreciate the interest of the SDOs for our work and our contributions, and we are willing to collaborate further with them. To be continued.

The SMESEC consortium launches a framework to protect SMEs against cyber incidents

May 27, 2020
FHNW

Madrid, May 27, 2020 – The SMESEC (Protecting Small and Medium-sized Enterprises digital technology through an innovative cyber-SECurity framework) consortium, coordinated by Atos Spain, released the first public version of the SMESEC Framework, a unified framework for Small and Medium-Sized Enterprises (SMEs). SMESEC helps SMEs to be protected against cyber-attacks and from the technical and awareness point of views.

Press Release ATOS: [link](#)
Press Release FHNW: [link](#)
Press Release GridPocket: [link](#)

The Cybersecurity Best Practices for SMEs Quiz

May 26, 2020
EGM



CYBERSECURITY SELF-ASSESSMENT

FOR SMALL AND MEDIUM BUSINESSES

Powered by  SMESEC  Cyber Security for Europe  Cyberwatching.eu  CYBERWISER.eu

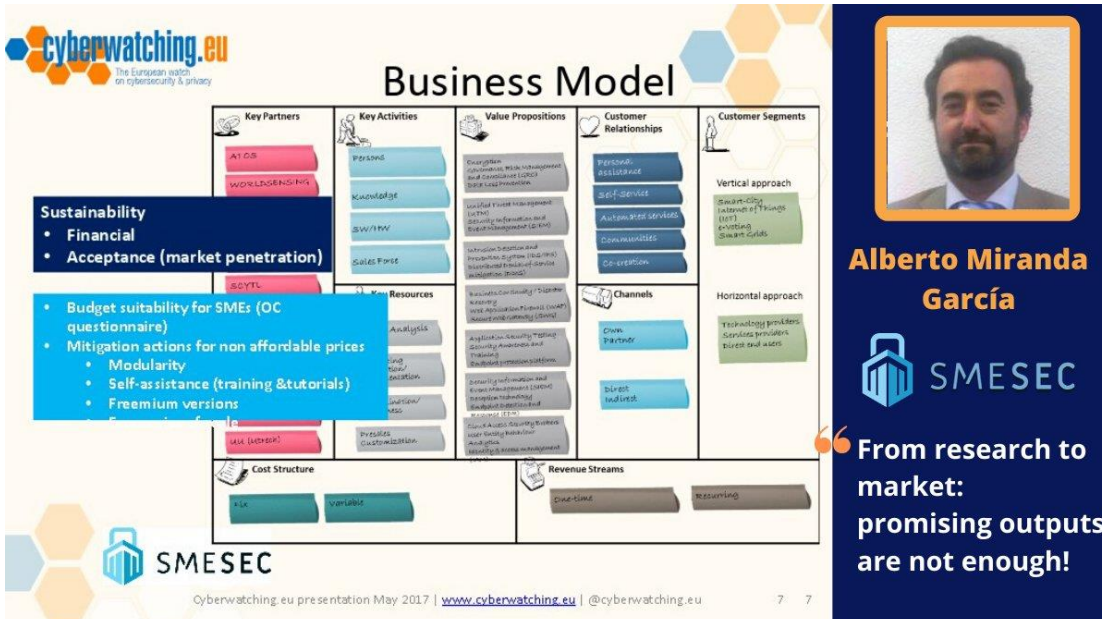
The "SME cybersecurity best practice quiz" was developed as a joint effort by four H2020 initiatives, namely CyberSec4Europe, Cyberwatching.eu, CYBERWISER.eu, and SMESEC. It is specifically designed to help companies' staff to increase awareness about basic security guidelines to be applied in their day-to-day routine. By answering a set of questions through a quick and straightforward online self-assessment, SMEs can easily understand where they stand in terms of their cybersecurity posture. The tool quickly helps SMEs to pinpoint security gaps and best practices that should be regularly followed through seven capabilities. The capabilities include Office Firewalls and Internet Gateways, Secure Configuration, Software Patching, User and Administrative accounts best practices, Malware protection, Awareness of Password weaknesses, and Basic risk assessment.

The "SME cybersecurity best practice quiz" is available free of charge and can be completed in less than 15 minutes. Measure your cybersecurity awareness skill, pinpoint your security gaps, and implement the best practices to avoid being a victim of a cyber-attack.

More information: <https://www.smesec.eu/smequiz.html>

3.3.2 Events

SMESEC at Cyberwatching.eu Webinar "From Research to Market, Promising Outputs are not Enough"



Business Model

Key Partners: ATOS, WORLENSENSING, SCYTL, USA (H2020)

Key Activities: Proposed, Knowledge, B2B/B2V, Gates Force

Value Propositions:

- Outcomes: risk reduction, multi-management, and continuous (CDD) data collection
- Useful tools: integration, L2/L3, security, forensics, and threat management (L2/L3)
- Information: detection and prevention, response, recovery, and incident response (IR)
- Business Case: Security, Disaster Recovery, Incident Response, Forensic (L2/L3), and threat management (L2/L3)
- Application: Security, Threat Security, Analytics, and Threat Intelligence (L2/L3)
- Security: Information and Event Management (L2/L3), Incident Response, and Threat Intelligence (L2/L3)
- Security: A large Security framework (L2/L3), Incident Response, and Threat Intelligence (L2/L3)

Customer Relationships: Personal, self-service, Automated services, Communities, Co-creation

Customer Segments:

- Vertical approach: Smart-City, Internet of Things (IoT), e-Health, Smart Grids
- Horizontal approach: Technology providers, Service providers, Retail and users

Channels: Own, Partner, Direct, Indirect

Cost Structure: Fixed, Variable

Revenue Streams: One-time, Recurring

Sustainability:

- Financial
- Acceptance (market penetration)

Mitigation actions for non affordable prices:

- Modularity
- Self-asistance (training & tutorials)
- Freemium versions

Alberto Miranda García

From research to market: promising outputs are not enough!

cyberwatching.eu presentation May 2017 | www.cyberwatching.eu | @cyberwatching.eu

On March 11, Atos participated in the “From Research to Market: Promising Outputs are not Enough!” webinar in Cyberwatching.eu (the European watch on cybersecurity and privacy). This webinar focused on improving project market readiness topics to identify the timing for project exploitation. In the webinar, three H2020 projects (PROTECTIVE, GHOST, and SMESEC) shared their knowledge and findings.

Alberto Miranda Garcia (Senior Business Consultant at Atos) presented the SMESEC framework, project partners, open call partners, the generation of the business model, and the findings of the project from the exploitation perspective. Knowledge-sharing and interaction with H2020 projects can provide SMESEC with opportunities for future improvement.

More information: <https://www.cyberwatching.eu/research-market-promising-outputs-are-not-enough>

The Last SMESEC Open Call Meeting

FORTH_Hellas organised the last SMESEC physical Open Call meeting in Amsterdam on February 4, 2020. Selected SMEs through the SMESEC Open Call participated in the validation workshop to share their findings and results of validation with SMESEC project partners.

For SMESEC, achieving a full validation of all the features provided by the framework is essential. During the meeting, Open Call partners had enough time to present the results of the validation and clarify their viewpoints. The validation results make a valuable contribution to SMESEC improvement.

More information: <https://www.smesec.eu/opencall.html>



SMESEC at the International Cybersecurity Forum (FIC2020)

As decided in the dissemination strategy (See D6.4) we found a big Cybersecurity related event in the 3rd period to show the SMESEC framework and get feedback from SMEs.

We decided to go to the International Cybersecurity Forum , a big event called FIC 2020 held in Lille from 28 to 30 visitors (see <https://www.forum-fic.com/en/home.htm>



The International Cybersecurity Forum (FIC) is the leading European event on Cybersecurity. The event relies on: a TRADE SHOW for buyers and suppliers of cybersecurity solutions to meet and network and a FORUM to foster reflection and exchanges among the European cybersecurity ecosystem. The International Cybersecurity Forum, place for open discussions and debate, welcomed in 2020 more than 450 speakers, through 4 plenary sessions, 33 round tables, 24 conferences, 35 technical demonstrations and 15 masterclass.!

This was a big opportunity for SMESEC to be present in an event which attracted +12500 visitors and 488 million of internet views

KEY FIGURES OF 2020 EDITION



12 500+
VISITORS



2 500
INTERNATIONAL GUESTS



110
COUNTRIES



90%
SATISFACTION RATE

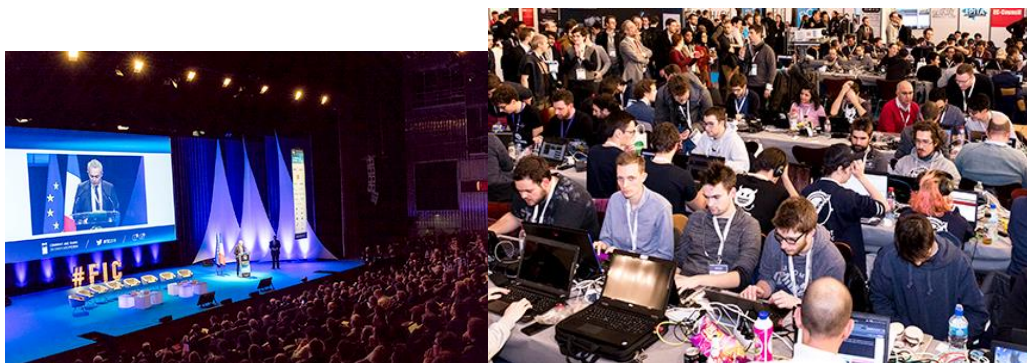
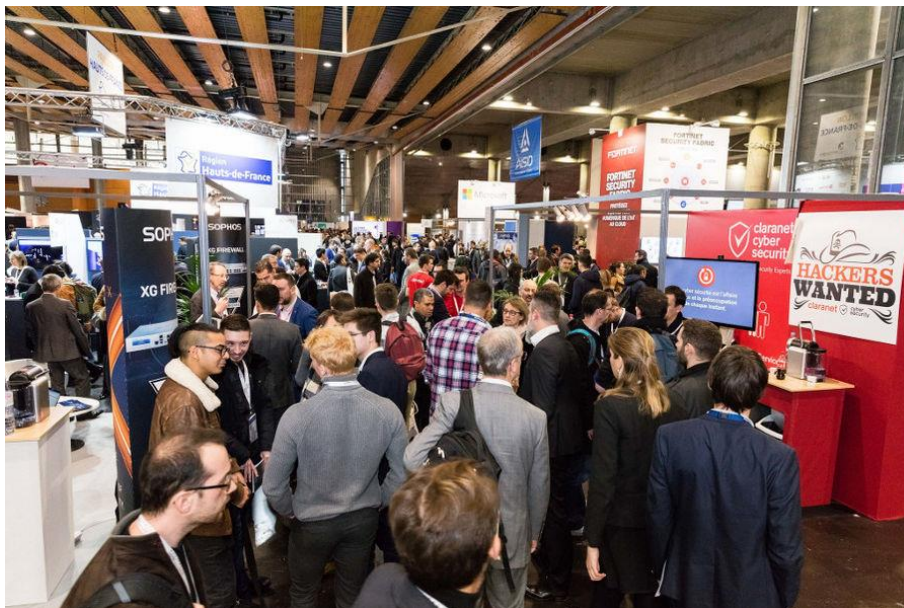


Figure 15: photos on showing massive attendance at FIC2020

SMESEC drove its presence and decided to contact 4 other EU partners to join forces to promote their offers to SMEs with the following messages:



Figure 16: design of the "wall" on the common EU Cybersecurity projects



Figure 17: P.Cousin and H. Baqua from EGM at SMEESEC booth, FI2020

At FIC we cooperate with 3 other EU projects as well as with Digital SME alliance

All three initiatives are tackling cybersecurity and privacy from complementary perspectives, providing European SMEs with key resources to boost their online security:

Cybersecurity Services & Tools for SMEs



These projects have received funding from the European Union's Horizon 2020 (H2020) Research and Innovation programme under Grant Agreements: CyberSec4Europe 830929; Cyberwatching.eu 740129; CYBERWISER.eu 786668; SMESEC 740787

Second SMESEC Workshop (IOSec- 2019)

September 26, 2019
FORTH



The second IOsec Workshop hosted in Luxembourg on September 26-27, 2019. The workshop brought together various viewpoints for advancing the practice of IT and OT security protection and improving security solutions for SMEs.

For SMESEC, the workshop offered the opportunity of networking, feedback, and discussion of the SMESEC framework. Also, during the workshop, SMESEC partners' papers with a SMESEC acknowledgment were presented.

More information: <https://iossec2019.ics.forth.gr/>

SMESEC at NIS Summer School 2019

September 16, 2019
FORTH



6th Network and Information Security Summer School is hosted in Crete, Greece, 16 - 20 September 2019. The theme of the event for this year was "Security Challenges of Emerging Technologies." The event is managed by the European Union Agency for cybersecurity (ENISA) and the Foundation for Research and Technology - Hellas (FORTH) together. The event provides the possibility for the policymakers from the EU Member States and EU Institutions, decision-makers from industry, and researchers from the academic community to have dialogue and exchange their ideas and advancements.

SMESEC project has been presented in the poster session. Received feedback from cybersecurity experts and also SMEs during different meetings may help SMESEC to obtain an in-depth understanding of the challenges and solutions regarding SMEs' cybersecurity problems.

More information: <https://nis-summer-school.enisa.europa.eu/>

SMESEC at IEEE CAMAD 2019

September 11, 2019
Citrix



IEEE International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD) hosted in Limassol, Cyprus, on September 11-3, 2019. This year, the main focus of IEEE CAMAD was on Communication and Experimentation aspects of 5G Networking.

Our partner, Citrix, presented the SMESEC project to the participants of the workshop. Moreover, Christos Tselios gave a tutorial on Hammer network traffic generator, an internal Citrix tool that emulates realistic traffic behaviour. For SMESEC, the workshop represented a platform for dissemination, obtaining feedback, and opportunities for future joint activities.

More information: <https://camad2019.ieee-camad.org/>

The First SMESEC Open Call

*September 09, 2019
FORTH*



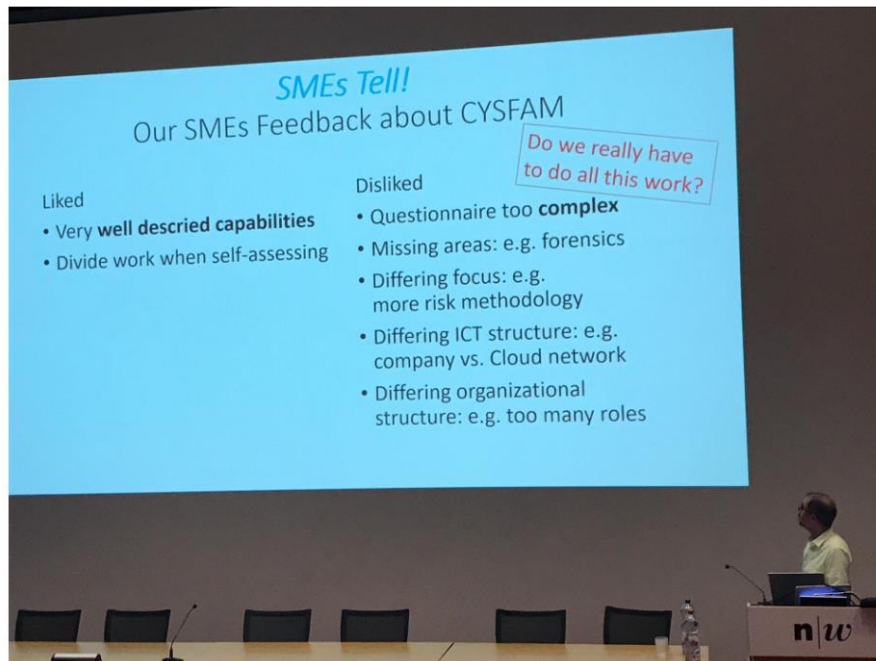
FORTH_Hellas organised the first SMESEC physical Open Call meeting in Heraklion on September 9-10, 2019. Seven SMEs selected through the SMESEC Open Call participated in the technical workshop to discuss SMESEC vision and validation with the project partners.

For SMESEC, achieving a full validation of all the features provided by the framework is essential. During the workshop, selected SMEs had several contacts with SMESEC partners and participated in several interviews.

More information: <https://www.smesec.eu/opencall.html>

SMESEC at IFIP Summer School 2019

August 19, 2019
FHNW



On August 19-23, FHNW presented a paper on the confidentiality of cybersecurity knowledge in SMEs in IFIP Summer School on Privacy and Identity Management hosted in Brugg, Switzerland. The goal of the IFIP summer school was to focus on the relationship between AI and privacy and attendees, overall, considered technical, legal, economic, and social science challenges.

For SMESEC, the event represented a platform for dissemination of the SMESEC project, discussing issues relevant to sharing cybersecurity information, and obtaining feedback about SMEs' confidentiality concerns.

More information: <https://www.ifip-summerschool.org/index.php/program/>

Swiss Cyber Think Tank

June 27, 2019
FHNW



Samuel Fricker participated at the Swiss Cyber Think Tank to explore recent developments in Switzerland in Cybersecurity. At the centre of the discussions were SME awareness and Skill development towards enabling cyber resilience and the political dialogue on expanding the reporting obligations for cyber incidents from critical infrastructure to SMEs.

For SMESEC, the participation allowed discussing the SMESEC vision and approach with the Swiss CERT agency, MELANI, and with diverse industrial players in the Swiss cybersecurity ecosystem, positioning SMESEC as an instrument to reinforce safety and trust in the Internet.

More information: <https://cyber-risk-insurance.com/scitl-events/>

SMESEC at the CONNECT University Summer School

June 24, 2019
Atos

From 24th of June until 5th of July 2019, the fourth edition of the CONNECT University Summer School (CUSS19) takes place, with cybersecurity as the overarching topic. It is a top-class learning opportunity, allowing participants to get cutting-edge insights on the technical, policy, economic, and societal aspects of cybersecurity and digital privacy. More than 35 high-level cybersecurity experts share their knowledge and innovative ideas and discuss upcoming cybersecurity challenges for Europe.

On June 28, Atos had a talk at the Summer School and presented SMESEC framework to the European Institutions' staff and cybersecurity experts. For SMESEC, this event represented opportunities for future joint activities to reinforce the securing of the European economy.

More information: <https://ec.europa.eu/futurium/en/connect-university/cybersecurity-risks-technology-driven-world>

Expert Workshop on Cybersecurity Skills for SMEs

June 21, 2019
FHNW



Samuel Fricker presented SMESEC-based skill development as the opening talk of the workshop on Skills for SMEs. The event under the patronage of the European Commission was hosted by the European Digital SME Alliance and moderated by CapGemini and involved more than twenty European experts with a wide diversity of views on connecting cybersecurity with SMEs.

For SMESEC, the participation allowed placing the SMESEC vision and approach on the European roadmap of skill development for SMEs. Also, the workshop allowed exploring current and future challenges of SMEs and understanding the current state-of-the-art, respectively avenues for future methods and solutions for allowing SMEs to become defenders of security.

More information: https://www.digitalsme.eu/digital/uploads/Workshop-21-June-2019_Invitation.pdf

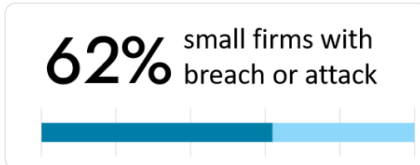
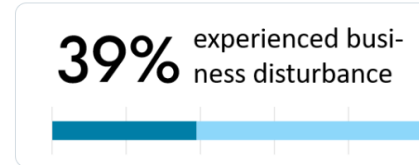
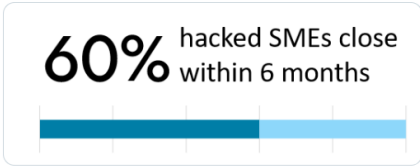




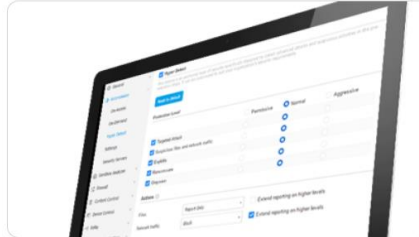
3.4 KPIs and Impact of SMESEC Dissemination




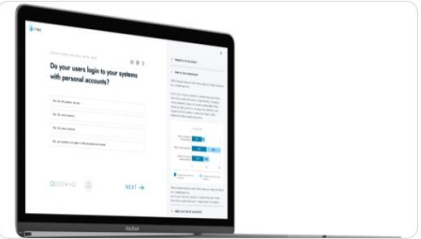







We have organized the SMESEC KPI along the funnel of raising awareness and interest and generating desire and action from SMEs and stakeholders towards the use and adoption of the SMESEC framework. This funnel is relevant for the SMESEC project as it represents the state-of-affairs for potential exploitation of the SMESEC framework at the end and after the project.

3.4.1 Awareness

Given the project's progress of implementing and piloting the SMESEC framework, dissemination could expand its social media posting with information about the SMESEC framework being released at the end of the project and the impact that this framework was offering during the pilots. Several content streams could be created and published to raise awareness about the SMESEC framework.

The following shows examples of campaigns with dedicated content streams:

Campaign, Outcomes Absolute (Average)	Examples
<p>Cybersecurity problem of SMEs</p> <p>29 Tweets, 7176 (247) Impressions, 215 (8) Interactions 851 impressions for: 62% small firms with breach or attack</p>	<div data-bbox="443 479 874 555"> <p>SMESEC @SMESEC_EU · May 17</p> <p>According to the UK Cyber Security Breaches Survey 2020, 62% of the small enterprises report having breaches or attacks in the last 12 months. Get secure. buff.ly/2YZBQMg #SMEs #Cybersecurity</p> </div> <div data-bbox="448 562 869 725">  <p>62% small firms with breach or attack</p> </div> <div data-bbox="879 479 1310 555"> <p>SMESEC @SMESEC_EU · May 20</p> <p>According to the UK Cyber Security Breaches Survey 2020, 19% of the attacked enterprises experienced a loss of money or data. 39% experienced business disturbances for the recovery. Get protected. buff.ly/2YZBQMg #SMEs #Cybersecurity</p> </div> <div data-bbox="884 562 1305 725">  <p>39% experienced business disturbance</p> </div> <div data-bbox="443 732 874 801"> <p>SMESEC @SMESEC_EU · May 14</p> <p>According to Cimcor, 60% of small companies close within 6 months of being hacked. buff.ly/2Bf0OpY Find protection with SMESEC smesec.eu #SMEs #Cybersecurity</p> </div> <div data-bbox="448 808 869 972">  <p>60% hacked SMEs close within 6 months</p> </div> <div data-bbox="879 763 1310 846"> <p>SMESEC @SMESEC_EU · May 20</p> <p>According to the UK Cyber Security Breaches Survey 2020, half of the businesses experience at least one breach or attack per month. For small firms, the average cost of a breach or attack is 1038€, for medium-sized 3469€. Budget your #CyberSecurity buff.ly/2YZBQMg #SMEs</p> </div> <div data-bbox="884 853 1305 972">  <p>12'456€ for a small firm per year</p> </div>
<p>SMESEC Framework: safeguard the SME with technical controls</p> <p>15 Tweets, 5766 (384) Impressions, 155 (11) Interactions 1295 impressions for: SMESEC framework positioning</p>	<div data-bbox="443 1003 874 1061"> <p>SMESEC @SMESEC_EU · May 25</p> <p>The SMESEC Hub: know with one glance how secure your #SME is and how to improve its security. #CyberSecurity</p> </div> <div data-bbox="448 1068 869 1301">  </div> <div data-bbox="879 978 1310 1061"> <p>SMESEC @SMESEC_EU · May 28</p> <p>The @IBM AntiROP Compiler Plugin allows compiling a C/C++ program with binary shuffling. AntiROP allows you to generate many versions of your executable, making your software costly to attack. buff.ly/2LxW1k #SMEs #CyberSecurity</p> </div> <div data-bbox="884 1068 1305 1301">  </div> <div data-bbox="443 1323 874 1375"> <p>SMESEC @SMESEC_EU · May 27</p> <p>Monitor your network and traffic with the @citrix Application Delivery Controller.</p> </div> <div data-bbox="448 1382 869 1617">  </div> <div data-bbox="879 1308 1310 1375"> <p>SMESEC @SMESEC_EU · May 20</p> <p>SMESEC GravityZone from @Bitdefender gives #SMEs a unified approach to security management. It offers comprehensive security and efficient management for the SME's endpoints. buff.ly/2LxW1k #CyberSecurity</p> </div> <div data-bbox="884 1382 1305 1617">  </div>

<p>SMESEC Framework: How to build strong security culture</p> <p>11 Tweets, 1910 (174) Impressions, 68 (6) Interactions 370 impressions for: CYSEC tool</p>	<p>SMESEC @SMESEC_EU · May 30 Nurture interest in #CyberSecurity by offering your most skilled and intrinsically interested employees high-quality learning. They will develop to becoming a role model and get the recognition for what it takes to be your Chief Information Security Officer #CISO #SMEs</p>  <p>SMESEC @SMESEC_EU · May 29 Integrate lessons from attacks, incidents, and #cybersecurity in your organisational memory together with your employees. Let employees share and discuss experiences so that they learn personally how to appraise threats and the effect of controls and behaviour. #SMEs</p>  <p>SMESEC @SMESEC_EU · May 28 Securityaware.me offers training for a wealth of important #CyberSecurity topics. #SMEs</p>  <p>SMESEC @SMESEC_EU · 20h The SMESEC Cybersecurity Coach #CYSEC guides your #CISO in self-assessing and improving the #CyberSecurity your #SME.</p> 
<p>Visibility of partners</p> <p>13 Tweets, 3742 (288) Impressions, 122 (9) Interactions 1399 impressions for: IBM partner</p>	<p>SMESEC @SMESEC_EU · May 29 Thank you @UtrechtUni for the insightful 3 years of building #CyberSecurity for #SMEs together leading to the SMESEC framework smesecc.eu</p>  <p>  Schweizerische Eidgenossenschaft Confédération suisse Confederazione Svizzera Confederaziun svizra</p> <p>This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 740787 (SMESEC). This work is supported by the Swiss State Secretariat for Education, Research and Innovation (SERI) under contract number 17.00067. The opinions expressed and arguments employed herein do not necessarily reflect the official views of these funding bodies.</p>
<p>Encourage interaction to stay in touch</p> <p>8 Tweets, 2993 (374) Impressions, 132 (17) Interactions 1485 impressions for: self-assessment</p>	<p>SMESEC @SMESEC_EU · May 31 The Cybersecurity Best Practices For SMEs Quiz bit.ly/3abxkhk</p>  <p>Trust-IT Services @TrustITServices · May 27 Very useful @cyberwiser @CyberSec4Europe @SMESEC_EU @cyberwatchingeu tool to help #SMEs assess their #cybersecurity skills! Take the Free assessment & get a certificate of completion issued by 4 #European projects! trust-it-services.com/news/smes-cybe...</p>  <p>SMESEC @SMESEC_EU · May 27 Cybersecurity Self-Assessment for Small and Medium-sized Businesses smesecc.eu/smequiz.html</p>  <p>SMESEC @SMESEC_EU · 11h Don't miss out on the latest information on Cybersecurity for SMEs. Sign up for the SMESEC Newsletter now. smesecc.atostoresearch.eu</p> 

According to the average indicators, the information about the cybersecurity problem of SMEs had reached the largest visibility, likely due to the large number of simple tweets that were published in this campaign. These tweets were a basis for motivating the technical controls and building of a strong cybersecurity culture supported by the social controls of the SMESEC framework. The technical controls raised about twice as much interested than the social

controls. The calls for interaction were most successful in generating conversions, encouraging readers to get to the SMESEC homepage.

The following shows the dissemination KPI related to generating awareness about SMESEC:

Channel	Target Y3	Achieved Y3
Twitter	19 posts per month	19.75 posts per month
Facebook	9 posts per month	9.5 posts per month
Linked-In	2 posts per month	5.67 posts per month
Project blog on Website with news and events	1 post per month	1.45 posts per month
Press releases	4 in total	5 in total
Participation at events	50 in total	41 in total

According to these KPI, the volume planned for dissemination for year 3 was achieved. As the illustrations from campaigns showed, the readiness of the SMESEC framework and the ongoing piloting in SMEs, which allowed us to gather lessons-learned, were enablers for the dissemination.

The schedule of event participation was well in line with the total ambition of the SMESEC project. However, due to the Covid-19 lock-down that started in February 2020, the events participations planned for Spring 2020 could not be realised until the end of the project in May 2020. The consortium used the released capacity to jointly author the SMESEC book.

3.4.2 Interest

The following shows the dissemination KPI related to third parties obtaining more information about SMESEC. The numbers exclude the visits of robots and attacks that were experienced.

Channel	Target Y3	Achieved Y3
Website visits per month	4000 per month	4301 per month
Website unique visitors per month	1000 per month	2282 per month
Downloads per month	83 per month	209 per month
Webinars	3 in total	2 in total
Tutorials	3 in total	7 in total
Magazine and newspaper articles	0 in total	2 in total (achieved in Y2 already)
Contributions to roadmaps	2 in total	1 in total
Contributions to standardisation	2 in total	2 in total
Contributions to policy	2 in total	0 in total

The webpage KPIs show that the SMESEC project succeeded to get more interest than originally anticipated. While the number of website visits was in line with the expectations, more than twice the number of expected unique visitors looked at the pages, and these visitors downloaded almost 3x as much material from the website than originally anticipated.

During the last project month, most interesting were the deliverables D2.1 SMESEC characteristics and market analysis (46 downloads), the SMESEC flyer (23 downloads), D6.1 dissemination plan and market analysis (22 downloads), and D2.3 the security awareness plan (21 downloads).

The consortium held a total of two webinars. The first was offered by FHNW focusing on cybersecurity for SMEs, and the second was offered by ATOS focusing on the SMESEC business model. The consortium prioritised the conclusion of the SMESEC framework development and reporting over holding an additional webinar.

To enable the work with the SMESEC framework, several tutorials were created and published on securityaware.me. They covered the ATOS tool XL-SIEM, FORTH Honeypots, Citrix ADC, FHNW CYSEC Cybersecurity Coach, EGM Test-as-a-Service, Bitdefender GravityZone, and IBM Anti-ROP Compiler Plugin.

SMESEC provided one contribution to a roadmap. FHNW participated in the Expert Workshop on Cybersecurity Skills for SMEs organised by Cap Gemini and Digital SME Alliance on behalf of the European Commission. The SMESEC framework and lessons were well received and considered in the definition of the roadmap. The Digital SME Alliance and Accountancy Europe followed up on this activity with cooperation that is building on the SMESEC results.

As described in Section 4.1 below, two contributions to standardisation were performed: one related to IoT security testing for ETSI ISG-CIM in September 2019 and one related to security assessment for ETSI TC CYBER in May 2020.

3.4.3 Desire

The following shows the dissemination KPI related to registrations:

Registrations	Target Y3	Achieved Y3
Twitter Followers	250	369
Facebook Followers	100	40
Linked-In Followers	100	92
SMESEC Framework	100 registrations	106 registrations
SMESEC Newsletter		12 registrations

According to these KPI, the Twitter channel bypassed our expectations. We received almost 50% more followers than originally planned. The website registrations and the Linked-In channel were within expectations. Facebook was not effective as a channel, and, in light that many other related EU initiatives are not present on Facebook, we discourage its use as a dissemination channel in future.

3.4.4 Action

The SMESEC framework has been in trial use by the following number of companies.

Trial Users	Target Y3	Achieved Y3
Use Case SMEs	4	4
Open Call SMEs	8	8

The SMESEC framework has not been offered as a product to the market yet. According to the SMESEC plan, this step is part of exploitation. For that reason, no statistics about sold licenses are provided here.

3.4.5 Scientific Dissemination

The SMESEC consortium reported the following scientific dissemination.

Trial Users	Target Y3	Achieved Y3
SMESEC workshops	2 in total	2 in total
Peer-reviewed journal publications	8 in total	3 in total

Peer-reviewed talks at conferences and workshops	20 in total	17 in total
1 PhD thesis	0 in total	1 in total

With the SMESEC workshop held in September 2019, the SMESEC consortium offered the scientific community a second opportunity to meet and discuss new knowledge and innovations related to cybersecurity for SMEs.

In total 3 out of 8 journal publications could be realised. At least one additional journal publication is in preparation but could not be submitted until the end of the project. Two partners signalled additional planned journal publications to be submitted after the project.

The schedule of talks for conferences and workshops was well in line with the total ambition of the SMESEC project. However, due to the Covid-19 lock-down that started in February 2020, the events and submission deadlines planned for Spring 2020 have shifted, and few publications could not be realised until the end of the project in May 2020. The consortium used the released capacity to jointly author the SMESEC book.

Dr. Hamza Baqa from Easy Global Market had successfully defended his thesis on “Realisation of Trust by a Semantic Self-Adaptation in the Internet of Things.” Aspects of this theses were introduced in the Testing-as-a-Service tool developed by Easy Global Market that is a component of the SMESEC framework.

4 Standardisation Activities

4.1 Collaboration with European Organisations and Standardisation Bodies

4.1.1 ENISA's Cybersecurity Standardization Conference 2020

On February 3 2020 in Brussels, the annual Cybersecurity Standardisation 2020 Conference organised by ENISA, ETSI, CEN and CENELEC was being held with around 400 participants: "Cybersecurity Standardization and the EU Cybersecurity Act - What's Up?". The standardisation task leader Marco Spruit participated in this conference.

The agenda, the names of the speakers and the presentations can be found on this web page.

https://www.enisa.europa.eu/events/cybersecurity_standardisation_2020/std-2020-presentations

A report is prepared about the conference and our takeaways is accessible on the following link:

<http://m.spru.it/news/smesec/cybersecuritystandardisation2020>

4.1.2 ETSI TC CYBER

As a follow-up to the [Cybersecurity Standardisation Conference 2020](#), Marco Spruit (the leader of the standardisation task in the SMESEC project) contacted the European Telecommunications Standards Institute (ETSI), which is one of the three standards developing organisations (SDOs) in Europe.

ETSI has a technical committee (TC) for cybersecurity, TC CYBER. Marco Spruit requested ETSI TC CYBER representatives to present the SMESEC project and the outcomes of the standardisation task (T6.3) in particular in a TC CYBER meeting. The presentation request was accepted and Marco Spruit was invited to present in the meeting that was held on May 19. The agenda of the presentation was as follows:

1. SMESEC introduction.
2. Cybersecurity for SMEs: From standardisation stakeholders workshop to research agenda.
3. <https://www.igi-global.com/article/cybersecurity-standardisation-for-smes/253856>
4. Cybersecurity standardization "where-to-start" guideline for European SMEs.
5. Cybersecurity maturity assessment of/for SMEs.
6. What's next?

Afterwards, the chair of the meeting requested feedback from all participants, which expressed their interest in the presentation, and the contributions of the standardisation task were well received. A follow-up collaboration has now been initiated specifically for the "Cybersecurity standardization "where-to-start" guideline for European SMEs".

4.1.3 CEN/CENELEC JTC 13

A CEN/CENELEC JTC 13 member was also present in the meeting and told the participants that the presented contributions to standardisation are very valuable and the SDOs should follow through. This CEN/CENELEC representative then requested the same presentation to be done in an upcoming CEN/CENELEC meeting.

We appreciate the interest from the SDOs for our work and our contributions and we are willing to collaborate further with them.

4.1.4 ETSI ISG-CIM

One of the SMESEC partners, EGM has contributed to ETSI ISG-CIM, the Industry Specification Group (ISG) cross cutting Context Information Management (CIM). The contribution is focusing on how to secure an "IoT context management API" at two levels: the first level is considering the API as web resource and the second one is dealing with the linked data and named graph. Hamza Baqa from EGM did a presentation on 12.09.2019 in an ETSI meeting.

4.2 Research Agenda: Cybersecurity Standardisation for SMEs

As reported in the previous annual report, an important accomplishment during the second year of the project was being able to get in touch with the key European standardisation bodies CEN, CENELEC and ETSI. As a result of our collaborations, we co-organised the workshop **Cybersecurity standards: what impacts and gaps for SMEs?** with StandICT.eu project. This workshop was reported in detail in the previous year's report.

Following this workshop, we wrote a paper to present our findings from the workshop to share them with the interested parties including SMEs, researchers, policy makers, SDOs and cybersecurity organisations. The aim of this paper was to give an understanding about what has been happening regarding cybersecurity standardisation for SMEs, specifically in Europe. Including the findings from the workshop and results from our literature searches, we propose an agenda for future research on cybersecurity standardisation for SMEs. We believe that this paper will shed light to the forthcoming research and innovation initiatives for SMEs' cybersecurity standardisation. The paper is titled "Cybersecurity Standardisation for SMEs: The Stakeholders' Perspectives and a Research Agenda" and was accepted for publication in the International Journal of Standardization Research (IJSR) Volume 17, Issue 2. Figure 18 shows a snapshot of the publisher's website for the paper. The paper is openly accessible via the following link: <https://www.igi-global.com/article/cybersecurity-standardisation-for-smes/253856>



Figure 18: Cybersecurity Standardisation for SMEs: The Stakeholders' Perspectives and a Research Agenda Paper

The following is the main research question (MRQ) that we address in this article:

“What are the gaps in cybersecurity standardisation for SMEs”

We break this main research question down into the following three sub research questions:

1. What are the trends in cybersecurity standardisation research for SMEs.
2. What are the experiences and views of the stakeholders on the gaps.
3. How can we distill from these 2 findings, new research questions for future research.

The first question is answered by a literature review, the second by the workshop findings, and the third question combines the literature and workshop findings. Figure 19 shows the research questions and their relations.

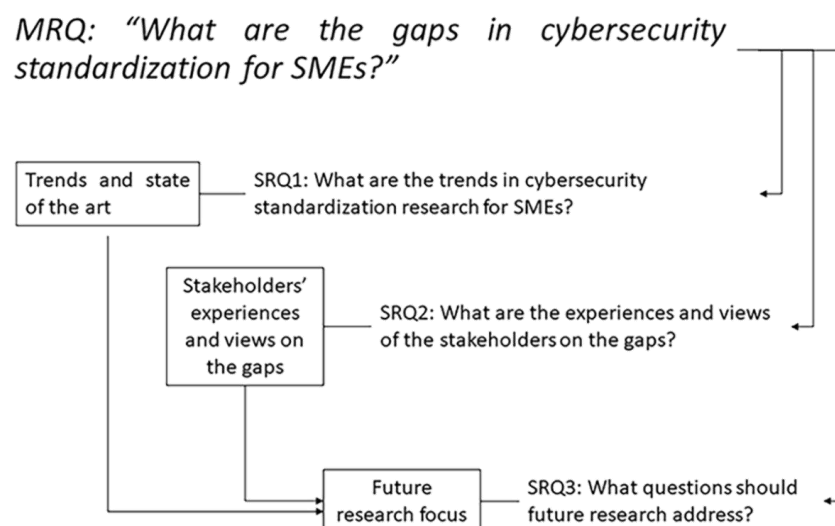


Figure 19: The research design of the paper "Cybersecurity Standardisation for SMEs "

In this paper, we have developed a research agenda for the coming years, for Cybersecurity Standardisation for SMEs and we formulated the 19 research questions shown in

Gaps and Research Questions	
<i>Gap 1: Lack of SMEs' awareness and involvement in standardisation processes</i>	
RQ 1.1	How can SMEs' awareness and involvement in cybersecurity standardisation be improved?
<i>Gap 2: Lack of cybersecurity standards specifically addressing SMEs</i>	
RQ 2.1	How can standards incorporate organisations' maturity levels?
RQ 2.2	How can SME-specific standards be developed?
RQ 2.3	How can organisational characteristics be used in developing standards specifically for SMEs?
RQ 2.4	How do SME cybersecurity requirements differ by their role in the digital ecosystem?
<i>Gap 3: Challenges of adapting existing cybersecurity standards for SMEs</i>	
RQ 3.1	How can maturity levels applicable to SMEs be introduced in standards?
RQ 3.2	What are the barriers for SMEs in adapting standards?
RQ 3.3	How can existing standards be adapted to SME characteristics?
RQ 3.4	How can organisational characteristics be used in adapting existing standards to SMEs?
RQ 3.5	To what extent the extensive number of cybersecurity standards raise a barrier for SME standardisation?
RQ 3.6	How can the need to converge toward useful, interoperable sets of standards be addressed?
<i>Gap 4: Financial barriers of available standards by SMEs</i>	
RQ 4.1	How can SMEs acquire standards and certifications at an affordable price?
RQ 4.2	To what extent do consultancy, implementation and maintenance costs influence SMEs uptake of standards and certifications?
<i>Gap 5: Lack of co-operation between the stakeholders</i>	
RQ 5.1	How can a direct link between EU funded research projects on cybersecurity and SDOs be established?

Figure 20: The 19 formulated research questions to steer future research on Cybersecurity Standardisation for SMEs.

4.3 Guideline: Cybersecurity Standardisation Essentials for European SMEs

In the SMESEC project, we have been working on cybersecurity standardisation and SME needs and requirements. We have investigated standards, important publications on cybersecurity standardisation. We have organized a workshop to bring SMEs, SDOs, and cybersecurity organisations together to find out the perspectives of the stakeholders and needs and gaps in cybersecurity standardisation for SMEs. We have also conducted research to identify the literature and the gaps in the literature regarding cybersecurity standardisation for SMEs. We have published a paper in IJSR journal to disseminate our findings as described in the previous section.

Having undertaken those initiatives, we decided to address SMEs in a guideline that presents the essentials on cybersecurity standardisation that we think are of their interest. We believe that this guideline will help SMEs to get started on their cybersecurity efforts.

Our approach in writing this guideline is holistic in the sense that it incorporates essentials for cybersecurity, cybersecurity standards and frameworks, how to use these standards and frameworks. We have taken the SME categories proposed by the Digital SME Alliance into account as described in section 3.4.2. This approach has brought us the opportunity to provide each category of SMEs focused information regarding their requirements.

Our Guideline provides a one-stop shop for this enormous target audience, and... “Keeps It Simple & Straightforward”.

1. First, we provide a *quick peek* on the barebones, essential, background information regarding SME Standardisation and the European Landscape.
2. Then, we describe in 5 easy steps, the *basic process* to establish and improve cybersecurity for SMEs.
3. For a start, within this process, an SME needs to understand their company profile.
4. Then, we present the *Top-5* cybersecurity frameworks and standards, which are relevant for SMEs, and compare them.
5. Finally, we present our *unified set of 17 security controls* from these Top 5 frameworks, as a one-stop-shop, **meta-best-practice** for SMEs to establish and improve their cybersecurity.

In the guideline, we provided a comparative analysis of five standards and frameworks that can be used for security controls by SMEs.

1. Cyber Essentials (UK),
2. The Centre for Cyber Security Belgium SME Guide (Belgium),
3. Center for Internet Security (CIS) (USA), ETSI TR 103 305-1 (Europe),
4. NIST Small Business Information Security (USA),
5. ISO/IEC 27002 Code of practice for information security controls (International).

We have selected these frameworks considering their country of origin, their applicability to SMEs and their scope of coverage with respect to security controls. Figure 21 shows the security controls presented in the guideline. In this table from the guideline, we also see the types of the security controls whether they are procedural, physical or technical.

Table 1. 17 Controls from five different standards and frameworks and their types

#	Control	Procedural	Physical	Technical
1	Management commitment and policies	X		
2	Asset Management	X	X	X
3	Patch Management	X		X
4	Access Control	X	X	X
5	Secure Computers, Servers and Network Configuration	X	X	X
6	Log Management	X		X
7	Email and Web Security	X		X
8	Malware Protection	X		X
9	Network and Communications Security	X		X
10	Back-up and Recovery Management	X		X
11	Data Protection and Encryption	X	X	X
12	Awareness and Training	X		
13	Secure Development	X		X
14	Incident and Continuity Management	X	X	X
15	Human Resource Security	X	X	
16	Improvement and Compliance	X		X
17	Supplier Relationships	X	X	X

Figure 21: Security Controls Presented in the Guideline

Figure 22 shows the comparative analysis of the Top 5 standards, from which we have derived the unified shortlist of 17 controls. The last column shown in Figure 22 directs SMEs to relevant standards specifically published for the given security control category.

Table 2 . Standards and Frameworks for Security Controls – A Comparative Analysis

#	Control/ Process	[1] Cyber Essentials (UK)	[2] The Centre For Cyber Security Belgium SME Guide (Belgium)	[3] Center for Internet Security (CIS) (USA) + ETSI TR 103 305-1 (Europe)	[4] NIST Small Business Information Security (USA)	[5] ISO/IEC 27002 Code of Practice for Information Security Controls	Additional Standards to Consider
1	Management commitment and policies		- Involving Top Management - Publish a Corporate Security Policy and a Code of Conduct		- Create policies and procedures for information security	6 Organizing information security 5 Information security policies	
2	Asset Management		- Manage Your Key ICT Assets	- Inventory and Control of Hardware Assets - Inventory and Control of Software Assets	- Identify what information your business stores and uses - Determine the value of your information - Develop an inventory - Dispose of old computers and media safely	8 Asset management	
3	Patch Management	- Patch Management	- Update All Programs	- Continuous Vulnerability Management	- Patch your operating systems and applications	12 Operations security	
4	Access Control	- Access Control	- Manage Access To Your Computers And Networks	- Controlled Use of Administrative Privileges - Controlled Access Based on the Need to Know - Account Monitoring and Control	- Use strong passwords - Limit employee access to data and information - Identify and control who has access to your business information - Require individual user accounts for each employee	9 Access control	
5	Secure Computers, Servers and Network Configuration	- Secure Configuration	- Secure Workstations and Mobile Devices - Secure Servers and Network Components	- Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers	- Use separate personal and business computers, mobile devices, and accounts - Do not connect personal or untrusted storage devices or hardware into your computer, mobile device, or network	12 Operations security 13 Communications security	
6	Log Management			- Maintenance, Monitoring and Analysis of Audit Logs	- Maintain and monitor logs	12 Operations security	
7	Email and Web Security			- Email and Web Browser Protections	- Set up web and email filters - Be careful downloading software - Watch for harmful pop-ups - Be careful of email attachments and web links - Conduct online business more securely	12 Operations security	
8	Malware Protection	- Malware Protection	- Install Antivirus Protection	- Malware Defenses	- Install and update anti-virus, -spyware, and other malware programs	12 Operations security	
9	Network and Communications Security	- Boundary firewalls	- Secure Servers And Network Components - Secure Remote Access	- Limitation and Control of Network Ports, Protocols, and Services - Secure Configuration for Network Devices, such as Firewalls, Routers and Switches - Boundary Defense - Wireless Access Control - Penetration Tests and Red Team Exercises	- Install and activate software and hardware firewalls on all your business networks - Secure your wireless access point and networks	13 Communications security	- ISO/IEC 27033 – Network security

Figure 22: Unified set of security controls for use by SMEs

The added value of Figure 22 can be found in the functional alignment of the relevant sections of the 5 aforementioned standards. This means that an SME who realises that they need to establish access control (which is control #4) can look up, with minimal effort:

- the section Access Control, in Cyber Essentials;
- the section Manage Access To Your Computers and Networks, in The Center For Cyber Security Belgium SME Guide;
- etc.

The guideline is under review to be a chapter of the SMESEC Book that will be published by Springer. We hope that this guideline will be considered as helpful and promoted by SDOs, SME organisations and cybersecurity organisations.

Finally, the main SME and cybersecurity organisations in the European landscape and Standards Developing Organisations (SDOs) are introduced in the guideline.

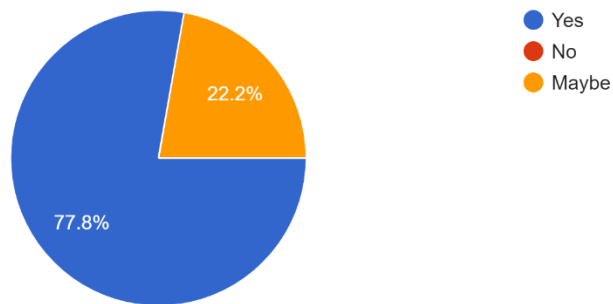
4.4 Results of the SMESEC Survey - Standardisation Related Questions

We have prepared a public SMESEC survey during the Open Call period that was filled in by 9 SMEs. In this survey, we also asked SMEs some questions about cybersecurity standards. In this section, we present the results as a summary.

Question 1: Do you believe that information security standards or cybersecurity standards may improve the quality of you services or products?

Do you believe that information security standards or cybersecurity standards may improve the quality of you services or products?

9 responses

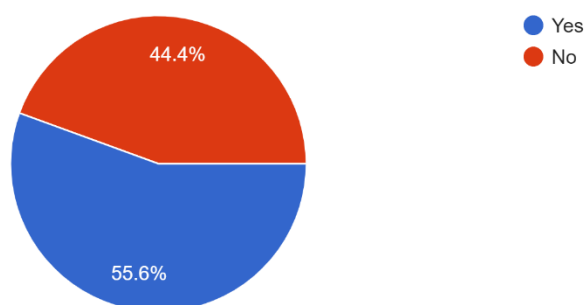


The result shown in the graph is positive in the sense that despite the challenges they face, SMEs believe that standards can improve their services and products. This shows that they are aware of the benefits of cybersecurity standardisation.

Question 2: Do you use any information security standards or cybersecurity standards in your business? If yes, which ones?

Do you use any information security standards or cybersecurity standards in your business? If yes, which ones?

9 responses



If yes, which ones?

4 responses

ISO

Different 3rd part tools, coding quality and derived security, but are also currently looking into ISO27001

the onces our it-partners demand for the integration

Cyberessentials is on the way

According to these results, the use of cybersecurity standards in the SMEs is not a common practice. The well-known standard from ISO is mentioned twice which is as expected. Another standard/framework mentioned is CyberEssentials that is more common in the UK.

Question 3: To what degree you agree with the following statements as barriers for using information security or cybersecurity standards.

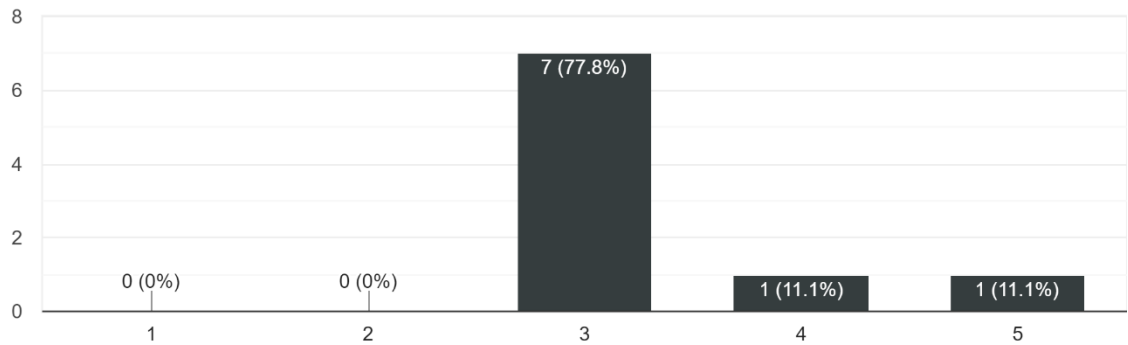
The following scale was used to collect the responses:

	1	2	3	4	5	
Strongly disagree	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	Strongly agree

Statement 1: There are too many standards. It is difficult to decide which ones to use.

There are too many standards. It is difficult to decide which ones to use.

9 responses

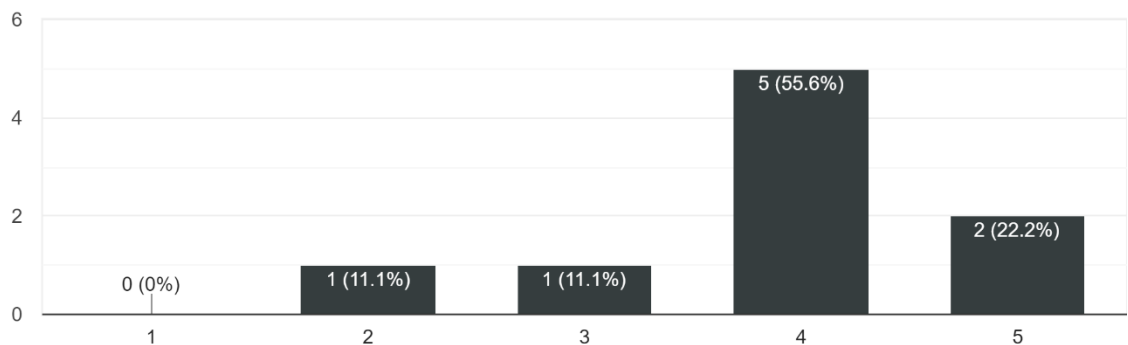


The results in this graph show that SMEs do not disagree with the statement. The majority of the responses are neutral, more than %22 of the SMEs agreed with the statement.

Statement 2: Standards are technically complex, not easy to understand or implement.

Standards are technically complex, not easy to understand or implement.

9 responses

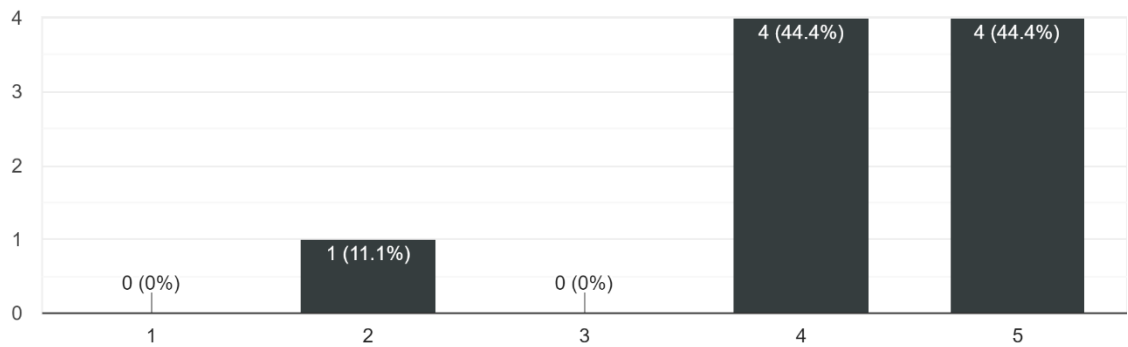


The results in this graph show that the majority of the SMEs (more than %77) agree with the statement. Only %11 of the SMEs do not agree that standards are technically complex, not easy to understand or implement.

Statement 3: Cost of acquiring standards is high.

Cost of acquiring standards is high.

9 responses

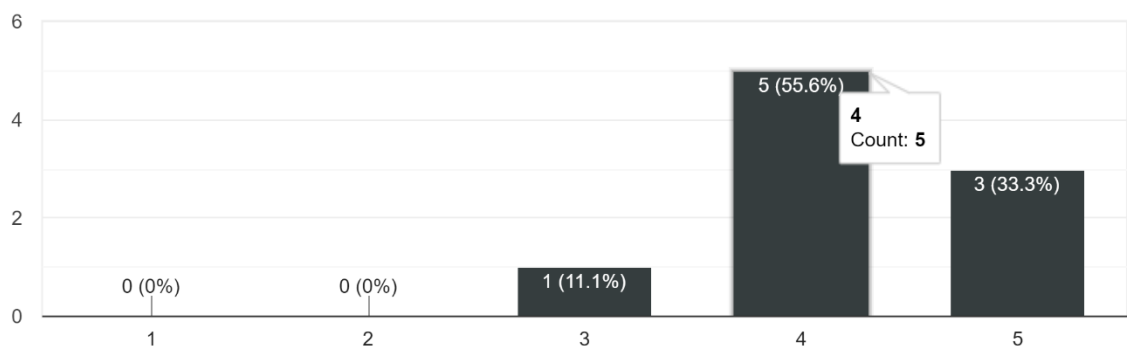


The results in this graph show that the majority of the SMEs (more than %88) agree that acquisition costs for standards are high.

Statement 4: Cost of implementing standards is high.

Cost of implementing standards is high.

9 responses

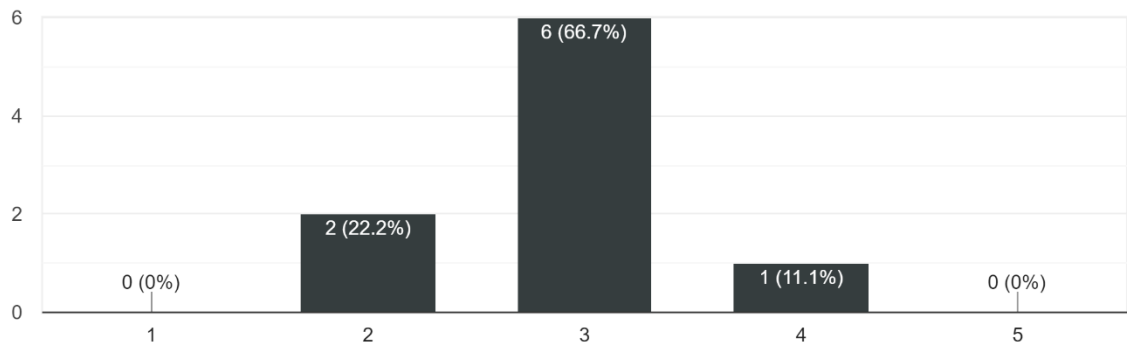


The results in this graph show that the majority of the SMEs (more than %88) agree that implementation costs for standards are high.

Statement 5: Benefits from implementing standards are unknown.

Benefits from implementing standards are unknown.

9 responses



The results in this graph show that the majority of the SMEs neither agree nor disagree that benefits from implementing standards are unknown. This is something needs to be taken into account by Standards Developing Organisations. The awareness of SMEs regarding the benefits of standards needs to be raised.

5 Conclusions

In the 3rd year the SMESEC framework was up and running. We therefore paid attention to promote the framework and get clear conditions to sell and exploit the project results.

We explored all business and legal conditions to exploit the framework with the partners and we checked the market interest and readiness to use full or part of the SMESEC framework. We have now set the conditions to promote the project results after the end of the project.

We disseminate the value of the SMESEC at face2face event such as big International Cybersecurity Forum FIC2020, at key workshop and with on-line dissemination actions such as mass mailing and survey. We checked then that SMESEC Framework has a strong interest from market players as made evidence by surveys and feedbacks at large events

Finally, we succeed to contribute to standardisation cooperating with key standardisation bodies such as CEN/CENELEC JTC 13 and ETSI TC CYBER. SMESEC contributes with a guide for SMEs which is going to be an ETSI Technical report according to members willingness expressed at last TC CYBER meeting in May 2020. This is a strong achievement.

6 References

- [1] [SMESEC, D2.1 SMESEC security characteristics description, security and market analysis report, George Oikonomou, 2017.
- [2] Independent, News <http://www.independent.co.uk/news/business/news/sme-cyber-protection-attacks-hackers-small-businesses-medium-sized-security-online-wannacry-a7868426.html>, retrieved date 2017-11-14
- [3] European Commission, Eurostat http://ec.europa.eu/eurostat/statistics-explained/index.php/ICT_security_in_enterprises, retrieved date 2017-11-14
- [4] ENISA, <https://www.enisa.europa.eu/publications/the-cost.../fullReport>, retrieved date 2017-11-14
- [5] European Commission, Cybersecurity fact sheet, <http://www.consilium.europa.eu/media/21480/cybersecurityfactsheet.pdf>, retrieved date 2017-11-14
- [6] European Commission, Cybersecurity fact sheet, <http://www.consilium.europa.eu/media/21480/cybersecurityfactsheet.pdf>, retrieved date 2017-11-14
- [7] CYBSAFE, Enterprise IT leaders demanding more stringent cyber security from suppliers, <https://www.cybsafe.com/en-gb/enterprise-it-leaders-demanding-more-stringent-cyber-security/>, retrieved date 2017-11-14
- [8] Small business trends, Cyber security statistics, <https://smallbiztrends.com/2017/01/cyber-security-statistics-small-business.html>, retrieved date 2017-11-14
- [9] Barclaycard, press-releases <https://www.home.barclaycard/media-centre/press-releases/small-businesses-failing-to-protect-themselves-from-growing-threat-of-cybercrime.html>, retrieved date 2017-11-14
- [10] MarketandMarket, Market-Reports http://www.marketsandmarkets.com/Market-Reports/cyber-security-market-505.html?gclid=EA1aIQobChMIwKbY14D_1gIVBRbTCh17XwdoEAAYASAAEgII2_D_BwE, retrieved date 2017-11-14
- [11] Wikipedia, Market segmentation, https://en.wikipedia.org/wiki/Market_segmentation, retrieved date 2017-11-14
- [12] European Commission, ANNUAL REPORT ON EUROPEAN SMEs https://ec.europa.eu/jrc/sites/jrcsh/files/annual_report_-_eu_smes_2015-16.pdf, retrieved date 2017-11-14
- [13] Symantec, Symantec report 2016: <https://www.symantec.com/content/dam/symantec/docs/reports/istr-21-2016-en.pdf>, retrieved date 2017-11-14

- [14] KBV Research, Europe IoT Data Management Market, <https://kbvresearch.com/europe-iot-data-management-market/>, retrieved date 2017-11-14
- [15] MarketsandMarkets, Market-Reports http://www.marketsandmarkets.com/Market-Reports/iot-data-management-market-53767032.html?gclid=EAIaIQobChMI1Y-vkMKY1wIVwZ0bCh21EQCxEAAYASAAEgLRvD_BwE, retrieved date 2017-11-14
- [16] Markets and Markets, Market-Reports https://www.marketsandmarkets.com/Market-Reports/user-entiy-behavior-analytics-market-76005696.html?gclid=EAIaIQobChMI7_aJnKHS1wIVVBobCh3y_QaNEAAYASAAEgLwLvD_BwE, retrieved date 2017-11-14
- [17] MarketandMarket, PressReleases,<https://www.marketsandmarkets.com/PressReleases/cloud-access-security-brokers.asp>, retrieved date 2017-11-14
- [18] MarketsandMarkets, Market-Reports https://www.marketsandmarkets.com/Market-Reports/endpoint-detection-response-market-261400972.html?gclid=EAIaIQobChMI08f4yqHS1wIVDI0bCh2foAKLEAAYASAAEgLatfD_BwE, retrieved date 2017-11-14
- [19] MarketsandMarkets, Market-Reports https://www.marketsandmarkets.com/Market-Reports/deception-technology-market-129235449.html?gclid=EAIaIQobChMImau64KHS1wIVQhbTCh3yOwMeEAAYASAAEgI03_D_BwE, retrieved date 2017-11-14
- [20] MarketandMarket, PressReleases,<https://www.marketsandmarkets.com/PressReleases/secure-web-gateways.asp>, retrieved date 2017-11-14
- [21] MarketsandMarkets, Market-Reports https://www.marketsandmarkets.com/Market-Reports/security-testing-market-150407261.html?gclid=EAIaIQobChMIIsYj6uqLS1wIV7hDTCh39qATuEAAYASAAEgIM9_D_BwE, retrieved date 2017-11-14
- [22] MarketandMarket, PressReleases,<https://www.marketsandmarkets.com/PressReleases/endpoint-security.asp>, retrieved date 2017-11-14
- [23] MarketsandMarkets, Market-Reports https://www.marketsandmarkets.com/Market-Reports/ddos-protection-mitigation-market-111952874.html?gclid=EAIaIQobChMIuKjPhaPS1wIVEWYbCh0dBQFqEAAYASAAEgK_6vD_BwE, retrieved date 2017-11-14
- [24] MarketandMarket, PressReleases,<https://www.marketsandmarkets.com/PressReleases/intrusion-detection-prevention-system.asp>, retrieved date 2017-11-14
- [25] PR Newswire, news-releases <https://www.prnewswire.com/news-releases/security-information-and-event-management-siem-market-worth--454-billion-by-2019-246872731.html>, retrieved date 2017-11-14

- [26] MarketandMarket, PressReleases, <https://www.marketsandmarkets.com/PressReleases/unified-threat-management.asp>, retrieved date 2017-11-14
- [27] MarketsandMarkets, Market-Reports https://www.marketsandmarkets.com/Market-Reports/enterprise-governance-risk-compliance-market-1310.html?gclid=EAIaIQobChMIgY6b2qPS1wIVyzLTCh3E-wc1EAAYASAAEgI2I_D_BwE, retrieved date 2017-11-14
- [28] Markets and Markets, Market-Reports https://www.marketsandmarkets.com/Market-Reports/identity-access-management-iam-market-1168.html?gclid=EAIaIQobChMiiJ7W6aPS1wIVUUhobCh3MTgNsEAAYAiAAEgIouvd_BwE, retrieved date 2017-11-14
- [29] European Commission, Energy, <https://ec.europa.eu/energy/en/topics/markets-and-consumers/smart-grids-and-meters>, retrieved date 2017-11-14
- [30] MarketandMarket, PressReleases, <https://www.marketsandmarkets.com/PressReleases/global-smart-grid.asp>, retrieved date 2017-11-14
- [31] Source: Internal creation of the consortium
- [32] MarketandMarket, PressReleases, <https://www.marketsandmarkets.com/PressReleases/iot-m2m.asp>, retrieved date 2017-11-14
- [33] Verizone, State of the Market: Internet of Things 2017 <http://www.verizonenterprise.com/verizon-insights-lab/state-of-the-market-internet-of-things/2017/>, retrieved date 2017-11-14
- [34] MarketandMarket, PressReleases, <https://www.marketsandmarkets.com/PressReleases/smart-cities.asp> retrieved date 2017-11-14
- [35] EY, Publications, [http://www.ey.com/Publication/vwLUAssets/ey-cyber-security-a-necessary-pillar-of-smart-cities/\\$FILE/ey-cyber-security-a-necessary-pillar-of-smart-cities.pdf](http://www.ey.com/Publication/vwLUAssets/ey-cyber-security-a-necessary-pillar-of-smart-cities/$FILE/ey-cyber-security-a-necessary-pillar-of-smart-cities.pdf), retrieved date 2017-11-14
- [36] King & Wood Mallesons, Who will lead Smart Cities - <http://www.kwm.com/en/hk/knowledge/insights/who-will-lead-smart-cities-20170523>, retrieved date 2017-11-14
- [37] Digital SME, <https://www.digitalsme.eu/about/european-digital-sme-alliance/>, retrieved date 2017-11-14
- [38] Mendelow, A. (1991) 'Stakeholder Mapping'.
- [39] e-voting.cc, Market Overview, <https://www.e-voting.cc/en/market-overview/>, retrieved date 2017-11-14

- [40] Ozkan, B., Lingen, S. van, & Spruit, M. (submitted). CYSFAM: The Cybersecurity Focus Area Maturity Model.
- [41] Bekkers, W., & Spruit, M. (2010). The Situational Assessment Method Put to the Test: Improvements Based on Case Studies. 4th International Workshop on Software Product Management (pp. 7–16). IWSPM, September 27, 2010, Sydney, Australia.
- [42] Eurosmart report
- [43] SMESEC consortium, D6.2 Annual report on exploitation, dissemination and standardization (Year 1), <https://www.smesec.eu/deliverables.html>
- [44] SMESEC consortium, D6.3 Annual report on exploitation, dissemination and standardization (Year 2), <https://www.smesec.eu/deliverables.html>
- [45] H2020 project Fortika, <https://fortika-project.eu>
- [46] Australian Cyber Security Growth Network, <https://www.austcyber.com/resources/sector-competitiveness-plan/chapter1/>, last time retrieved April 2020
- [47] IT Governace, <https://www.itgovernance.co.uk/>, last time retrieved may 2020
- [48] SMESEC consortium, D6.5 Business model definition, <https://www.smesec.eu/deliverables.html>
- [49] Fire eye, <https://www.fireeye.com/solutions/small-and-midsize-business.html>, last time retrieved April 2020
- [50] Comodo, <https://www.comodo.com/why-comodo.php?track=14955&af=14955>, last time retrieved April 2020
- [51] ESET, <https://www.eset.com/es/> last time retrieved April 2020
- [52] Cyberlarm, <https://www.cyberalarm.org/>, last time retrieved April 2020
- [53] Forbes, <https://www.forbes.com/sites/louiscolumbus/2020/04/05/2020-roundup-of-cybersecurity-forecasts-and-market-estimates/#59fdb4db381d>, last time retrieved April 2020
- [54] Small Biz Trends, <https://smallbiztrends.com/2019/09/2019-smb-it-security-report.htm>, last time retrieved April 2020
- [55] SMESEC consortium, D5.5 SMESEC Open call design, implementation and results report, <https://www.smesec.eu/deliverables.html>

7 Annexes

7.1 Annex I IPR Agreement

IPR AGREEMENT

BETWEEN:

Description of partners detailed in the Consortium Agreement

IPR AGREEMENT

BETWEEN:

Description of Parties detailed in the Consortium Agreement

1. ATOS SPAIN SA (ATOS), established in CALLE DE ALBARRACIN 25, MADRID 28037,

Spain, VAT number: ESA28240752, represented for the purposes of signing the Agreement by Alicia GARCÍA

2. WORLDSENSING S.L.N.E (WoS), established in C ARAGO 383, PLANTA 4, BARCELONA 08013, Spain, VAT number: ESB64902208,

3. PANEPISTIMIO PATRON (UoP), established in UNIVERSITY CAMPUS RIO PATRAS, RIO PATRAS 265 04, Greece, VAT number: EL998219694,

4. FOUNDATION FOR RESEARCH AND TECHNOLOGY HELLAS (FORTH), established in N PLASTIRA STR 100, HERAKLION 70013, Greece, VAT number: EL090101655,

5. EASY GLOBAL MARKET SAS (EGM), established in ROUTE DES LUCIOLES 2000 CS 90029 LES ALGORTIHMES BATIMENT A, BIOT 06410, France, VAT number: FR10524029469,

6. SCYTL SECURE ELECTRONIC VOTING SA (SCY), established in PLACA GAL LA PLACIDIA 1-3, 1A PLANTA, BARCELONA 08006, Spain, VAT number: ESA62604087,

7. GRIDPOCKET SAS (GRIDP), established in ROUTE DE CRETES 300, VALBONNE SOPHIA ANTIPOLIS 06560, France, VAT number: FR06518639695,

8. FACHHOCHSCHULE NORDWESTSCHWEIZ (FHNW), established in BAHNHOFSTRASSE 6, WINDISCH 5210, Switzerland, VAT number: CHE116216865MWST,

9. CITRIX ELLAS MONOPROSOPIETAIRIA PERIORISMENIS EVTHINIS (CITRIX), established in EO KATO-ANO KASTRITSIOU 4, KATO KASTRITSI PATRAS 26504, Greece, VAT number: EL099730753,

10. **IBM ISRAEL - SCIENCE AND TECHNOLOGY LTD (IBM)**, established in 94 DERECH EM-HAMOSHAVOT, PETACH TIKVA 49527, Israel, VAT number: IL95432408,
11. **BITDEFENDER SRL (BD)**, established in STRADA DELEA VECHE 24 CLADIREA DE BIROURI A ETAJ 7, BUCURESTI 62204, Romania, VAT number: RO18189442,
12. **UNIVERSITEIT UTRECHT (UU)**, established in HEIDELBERGLAAN 8, UTRECHT 3584 CS, Netherlands, VAT number: NL001798650B01,

hereinafter, jointly or individually, referred to as "Parties" or "Party" relating to the Action entitled

Protecting Small and Medium-sized Enterprises digital technology through an innovative cyber-SECurity framework

in short

SMESEC

hereinafter referred to as "Project" or "Action"

WHEREAS:

The Parties, having considerable experience in the field concerned and are conducting a Project to the Funding Authority as part of the Horizon 2020 – the Framework Programme for Research and Innovation (2014-2020).

The Parties wish to specify or supplement binding commitments regarding intellectually property rights (IPR) handling among themselves in addition to the provisions of the specific Grant Agreement and Consortium Agreement.

NOW, THEREFORE, IT IS HEREBY AGREED AS FOLLOWS:

1. Purpose

1.1 The purpose of this IPR Agreement is to specify with respect to the Project the IPR ownership of all software components developed within the Project.

1.2 The "SMESEC" Grant Agreement and the "SMESEC" Consortium Agreement are integral parts of this agreement and its content prevails should this agreement contain clauses contradicting them.

1.3 The agreements made herein settle only the purpose defined in section 1.1 and not any future contracts or contracts, which are currently negotiated between some Parties.

2. Definitions

The following terms have the meaning specified below.

Component: all software innovations developed during the project lifespan by one or several Parties and the background items they have dependences to.

Contributing Parties: means all Parties that have helped to the co- creation of a project component.

Framework: software development which implements a platform where the user information, and cybersecurity tools, services and Components developed by Parties, are integrated and hosted.

Framework Connector: software development where Parties allow access, via the Framework, to their Components.

Lead Developer. means the Party that has coordinated to the co- creation of one or several project components.

Intellectual Property Rights (hereinafter “IPRs”). means all trade secrets, patents and patent applications, trademarks (whether registered or unregistered including any goodwill acquired in such trademarks), service marks, trade names, business names, internet domain names, e-mail address name, copyrights (including rights in computer software), moral rights, database rights, design rights, rights in know-how, rights in confidential information, inventions (whether patentable or not) and all other intellectual property rights (whether registered or unregistered, and any application for the foregoing), and all other equivalent or similar rights which may be subject anywhere in the world

IPR %: Is understood as the distribution of the property of the IPRs among all Parties contributing to the development of one or several of the project components

Results: as defined in the Grant Agreement, means any (tangible or intangible) output of the action such as data, knowledge or information — whatever its form or nature, whether it can be protected or not — that is generated in the action, as well as any rights attached to it, including intellectual property rights.

3. IPR Ownership

Section 8 and specifically subsections 8.0 and 8.1 of the “SMESEC” Consortium Agreement settle the ownership of Results.

In addition to the Consortium Agreement, this document settles that “*generation of results*” means that an owner has developed specific software components through substantial effort, research, time, and expense.

Basically, Results are owned by the Party that generates them. However, if results are jointly generated and if it is not possible to establish the respective contribution of each Party; or separate them for the purpose of applying for, obtaining or maintaining their protection, a joint ownership is the case.

The following table lists all resulting Components generated in the SMESEC project and indicates whether:

- the Component is owned by a single Party or

- in case of joint ownership
 - the Component is owned by multiple Parties and contributions are separable or
 - if the Component cannot be separated the degree (%) of a Party's ownership

If a listed Component uses (binary) code from another listed Component, this code IS NOT covered by the corresponding IPR assignment.

Name of Component	Lead developer	Contributing parties	IPR %
IBM Virtual patch			
	IBM		100%
Risk Assessment Engine (RAE)			
	ATOS		100%
EGM-TaaS			
	EGM		100%
Anti-Rop			
	IBM		100%
Testing Platform (ExpliSAT)			
	IBM		100%
Citrix ADC			
	CITRIX		100%
Citrix ADC aggregator			
	CITRIX		100%
Cross-layer SIEM (XL-SIEM)			
	ATOS		100%
End Point Protection Platform			
	BD		100%
EWIS (Early Warning Intrusion Detection)			
	FORTH		100%
Dionaea(GPLv2)	FORTH		100%
IoTHoneypot (3-Clause BSD)	FORTH		100%
Kippo (3-Clause BSD)	FORTH		100%
DDoS Tool(GPLv2)	FORTH		100%
Cloud-based IDS (Intrusion Detection System)			
	FORTH		100%

Name of Component	Lead developer	Contributing parties	IPR %
SNORT(GPLv2)			
CYSEC			
CYSEC Framework	FHNW	-	100%
CYSEC Coaches			
Company Coach	FHNW	UU	50%
User Training Coach	FHNW	UU	50%
Patch Management Coach	FHNW	UU	50%
Access Control Coach	FHNW	UU	50%
Malware Coach	FHNW	UU	50%
Backup	FHNW	UU	50%
Maturity Model	UU		100%
Trainig platform			
	UoP		100%
SMESEC Hub			
	WoS		100%
FORTH Framework Connector			
	FORTH		100%
EGM Framework Connector			
	EGM		100%
BD Framework Connector			
	BD		100%
IBM Framework Connector			
	IBM		100%
Framework			
Framework backend (Business logic + application support + authentication)	ATOS		100%
Framework user interface (Design -images- + html, css and js files)			
	FHNW		70%
	ATOS		30%

Date: DD.MM.YYYY

Name:

Function:

Representing the following body:

full official address, and if any, VAT/registration number

Signature:

7.2 Annex II Exploitation agreement

Exploitation Agreement

Version 0.5

SMESEC



SMESEC

Protecting Small and Medium-sized Enterprises digital technology through an innovative
cyber-SECurity framework

This Exploitation Agreement (the “**Agreement**”) is made on **25/05/2020**:

BETWEEN:

1. **ATOS SPAIN SA** , established in CALLE DE ALBARRACIN 25, MADRID 28037, Spain, represented for the purposes of signing the Agreement by Alicia GARCÍA
2. **WORLDSENSING S.L.**, established in C VIRIAT 47 PLANTA 10, BARCELONA 08014, Spain, represented for the purposes of signing the Agreement by Ignasi VILAJOSANA
3. **PANEPISTIMIO PATRON**, established in UNIVERSITY CAMPUS RIO PA-TRAS, RIO PATRAS 265 04, Greece, represented for the purposes of signing the Agreement by
4. **FOUNDATION FOR RESEARCH AND TECHNOLOGY HELLAS**, established in N PLASTIRA STR 100, HERAKLION 70013, Greece, represented for the purposes of signing the Agreement by
5. **EASY GLOBAL MARKET SAS**, established in ROUTE DES LUCIOLES 2000 CS 90029 LES ALGORTIHMES BATIMENT A, BIOT 06410, France, represented for the purposes of signing the Agreement by
6. **SCYTL SECURE ELECTRONIC VOTING SA**, established in PLACA GAL LA PLACIDIA 1-3, 1A PLANTA, BARCELONA 08006, Spain, represented for the purposes of signing the Agreement by
7. **GRIDPOCKET SAS**, established in ROUTE DE CRETES 300, VAL-BONNE SOPHIA ANTIPOLIS 06560, France, represented for the purposes of signing the Agreement by
8. **FACHHOCHSCHULE NORDWESTSCHWEIZ**, established in BAHNHOFSTRASSE 6, WINDISCH 5210, Switzerland, represented for the purposes of signing the Agreement by
9. **CITRIX ELLAS MONOPROSOPIETAIRIA PERIORISMENIS EVTHINIS**, established in EO KATO-ANO KASTRITSIOU 4, KATO KASTRITSI PATRAS 26504, Greece, represented for the purposes of signing the Agreement by
10. **IBM ISRAEL - SCIENCE AND TECHNOLOGY LTD**, established in 94 DERECH EM-HAMOSHAVOT, PETACH TIKVA 49527, Israel, represented for the purposes of signing the Agreement by
11. **BITDEFENDER SRL**, established in STRADA DELEA VECHE 24 CLADI-REA DE BIROURI A ETAJ 7, BUCURESTI 62204, Romania, represented for the purposes of signing the Agreement by
12. **UNIVERSITEIT UTRECHT**, established in HEIDELBERGLAAN 8, UTRECHT 3584 CS, Netherlands, represented for the purposes of signing the Agreement by

Being referred, individually, to a “Party” or collectively the “Parties”,

relating to the exploitation of the results of the project entitled “**SMESEC**” (the “**Project**”) content co-funded by the European Commission in the scope of the H2020 programme, under the Grant Agreement No740787 (the “**Grant Agreement**”), and regarding which the Parties have entered into the consortium agreement dated 22/05/2017 (the “**Consortium Agreement**”).

Table of Contents

Document Information	2
Table of Contents	3
List of Tables.....	5
List of Figures	6
List of Acronyms.....	7
Executive Summary	9
1 Introduction.....	10
1.1 Purpose of the document	10
1.2 Relation to other project work.....	10
1.3 Structure of the document	10
2 Exploitation Activities	11
2.1 Exploitation Strategy	11
2.1.1 Joint Exploitation Plan	12
2.1.2 Individual Exploitation.....	15
2.1.3 Exploitation next step after the project end.....	24
2.2 Business Plan.....	26
2.2.1 Summary.....	26
2.2.2 Market Monitoring	26
3 Project dissemination	2
3.1 Dissemination strategy	2
3.1.1 Global approach and phasing	2
3.1.2 Objectives.....	3
3.1.3 Targets.....	4
3.1.4 Dissemination Messages	5
3.2 SMESEC Dissemination Highlights.....	6
3.2.1 SMESEC Survey V2.0	6
3.2.2 Feedback about Suitability of SMESEC Approach from Public Administration..	8
3.2.3 Quiz on Cybersecurity Best Practices for SMEs.	10
3.2.4 SMESEC Book.....	11
3.2.5 Press Releases about the SMESEC Framework Release.....	12
3.3 News and Events	15
3.3.1 News.....	16
3.3.2 Events	16
3.4 KPIs and Impact of SMESEC Dissemination	27

3.4.1	Awareness.....	27
3.4.2	Interest.....	30
3.4.3	Desire.....	31
3.4.4	Action.....	31
3.4.5	Scientific Dissemination.....	31
4	Standardisation Activities.....	33
4.1	Collaboration with European Organisations and Standardisation Bodies.....	33
4.1.1	ENISA's Cybersecurity Standardization Conference 2020.....	33
4.1.2	ETSI TC CYBER.....	33
4.1.3	CEN/CENELEC JTC 13.....	34
4.1.4	ETSI ISG-CIM.....	34
4.2	Research Agenda: Cybersecurity Standardisation for SMEs.....	34
4.3	Guideline: Cybersecurity Standardisation Essentials for European SMEs.....	36
4.4	Results of the SMESEC Survey - Standardisation Related Questions.....	39
5	Conclusions.....	45
6	References.....	46
7	Annexes.....	50
7.1	Annex I IPR Agreement.....	50
7.2	Annex II Exploitation agreement.....	56
7.3	Annex III SMESEC- Letter of intent.....	14

1. Definitions

Words with capital letters which are not defined in this Agreement shall have the same definition as those provided in the Consortium Agreement.

In this Agreement, the following words shall have the meaning determined hereunder:

“**Assets**” means any project result designed as such by the project partners, such as Methods, Algorithms, Reference Architectures, Software Platforms and Components as well as their instantiations into several Industrial Trials experimentations. A complete list of Assets generated during the project is included in ANNEX I: Assets.

“**Business Opportunity Dossier**” is a document prepared by the Contractor Party describing as many details as possible related to the specific Business Opportunity, including proposed offering with related Assets and Services, draft financial conditions, list of Concerned Parties and any other that Lead Generator considers important to realize the opportunity.

“**SMESEC Licence**” means a licence that will be defined by the Consortium during the Project.

“**Commercial Business Opportunities or shortly Business Opportunity (BO)**” means that one of the Parties has the opportunity to sell Assets or Product to a final customer on the market, which is not any of the Party that signed this agreement.

“**Concerned Parties**” are all Parties that have been identified by the Contractor in the Business Opportunity Dossier as IP Owners or Service Providers.

“**Contractor Party**” is the Party that carries out activities related to the preparation of commercial offering based on the Product, including the preparation of business opportunity dossier and actually signs contract with the customer and takes responsibility of revenue sharing as agreed in this agreement.

“**Implementation Arrangements**” are any further agreements, contracts or similar that are used after the preparation of the Final Business Opportunity Dossier in order to realize this opportunity.

“**Intellectual Property Owner (IP Owner)**” is the Party that partially or totally owns IP over an Asset as listed in the ANNEX II: IP Sharing

“**Internal Use Opportunity**” means that one of the Parties (or an entity that belongs to the same Group of the Party) is the final customer for the Assets or Products or intends to apply Assets or Products for its own activities.

“**Lead**” is the potential final customer contact information and in some cases, more detailed information of a potential customer (e.g. budget).

“**Lead Generator**” means the Party that has initial contacts with a potential customer and that answers initial enquiry into Assets or Products defined in this agreement.

“**Party**” or “**Parties**” means a party or the parties that have signed the present Exploitation Agreement.

“**Revenue**” is the income received by the Parties for the BO, after the deduction of the costs incurred by the Parties in the implementation of the BO and it refers value before the taxes.

“**The Product**” means the SMESEC Framework. It is the results of the SMESEC project that brings together the three (3) assets developed by the signing parties during the project as detailed in ANNEX I: Assets.

2. Scope

In the context of the Project, the Parties have produced results in the form of a range of separately exploitable components. All components have been produced by one sole Party.

The purpose of this Agreement is to establish the terms under which the Parties will exploit Commercial Business or Internal Use Opportunities derived from the commercialisation of The Product, once the EU co-financed Project is finalised.

3. Duration

This Agreement shall take effect on the date hereof and remain valid until the expiration of a period of twelve (12) months from the date on which the Grant Agreement is terminated (the “Final Date”), and shall be thereafter renewed for one (1) year periods, each Party being entitled to terminate its participation, after the Final Date, at any moment by sending to the other Parties a termination notice in this respect, which shall take effect at least sixty (60) days after the date of the termination notice.

Notwithstanding anything to the contrary, in case of termination, the rights and obligations deriving from this Agreement will be maintained until finalisation of all Business Opportunities for which the rights have been granted before termination carried out by one or more of its Parties in accordance with the conditions provided therein.

4. Exploitation Committee

a. Exploitation Coordination Committee

The exploitation Coordination Committee (“ECC”) is the main entity which will be in charge of the exploitation of the Product(s).

The ECC will be composed of one representative of each Party. The ECC shall appoint the representative of ATOS as the Chairman until the first meeting.

Parties	ECC Representative
ATOS SPAIN SA	
WORLDSENSING S.L.	Andrea Bartoli
PANEPISTIMIO PATRON	
FOUNDATION FOR RESEARCH AND TECHNOLOGY HELLAS	
EASY GLOBAL MARKET SAS,	
SCYTL SECURE ELECTRONIC VOTING SA	
GRIDPOCKET SAS	
FACHHOCHSCHULE NORDWESTSCHWEIZ	
CITRIX ELLAS MONOPROSOPIETAIRIA PERIORISMENIS EVTHINIS	
IBM ISRAEL - SCIENCE AND TECHNOLOGY LTD,	
BITDEFENDER SRL	
UNIVERSITEIT UTRECHT	
TOTAL	12

After having informed the others in writing, each Party shall have the right to replace its representative and/or to appoint a proxy although it shall use all reasonable endeavors to maintain the continuity of its representation.

The voting power shall have the following distribution once the Project has finished, which is foreseen by 01/06/2020:

Parties	Votes
ATOS SPAIN SA	1
WORLDSENSING S.L.	1
PANEPITIMIO PATRON	1
FOUNDATION FOR RESEARCH AND TECHNOLOGY HELLAS	1
EASY GLOBAL MARKET SAS,	1
SCYTL SECURE ELECTRONIC VOTING SA	1
GRIDPOCKET SAS	1
FACHHOCHSCHULE NORDWESTSCHWEIZ	1
CITRIX ELLAS MONOPROSOPIETAIRIA PERIORISMENIS EVTHINIS	1
IBM ISRAEL - SCIENCE AND TECHNOLOGY LTD,	1
BITDEFENDER SRL	1
UNIVERSITEIT UTRECHT	1
TOTAL	12

A quorum shall be formed by a minimum of 50% of the votes +1. Where decisions are to be taken unanimously, all Parties must be represented at the meeting.

Decisions shall be taken by the majority of the votes of the Parties present or represented by proxy at a quorum meeting, always provided that any Party, whose rights or liabilities are changed, may veto such decisions.

b. ECC main responsibilities

- i. Making proposals to the Parties for the review and/or amendment of the terms of the Exploitation Agreement.
- ii. Establishment of a Business Opportunity Committee (BOC) for the identified Business Opportunities. The BOC will be composed of one representative of each of the Parties involved in the Business Opportunity. The Lead Generator will inform the ECC once a new BO is available in order to create a BOC to manage the opportunity.
- iii. Defining new types of roles for the Parties (or modifying the current definitions) as well as their associated rights and obligations.
- iv. Updating the roles performed by each Party.
- v. Making proposals to the Parties (other than the Defaulting Party) to service of notices on a Defaulting Party and where applicable, to assign the Defaulting Party's tasks to specific entity(ies), preferably chosen from the remaining Parties.
- vi. Links with other organizations within and outside Europe in order to:
- vii. identify possible distributors and customers
- viii. identify possible strategic alliances with other organizations for future deployment
- ix. Links with existing and future technology providers.
- x. Coordinate marketing actions.

5. Results of the Project

The Parties agree that the list of project results designated as Assets, as well as intellectual property (IP) ownership of the Assets shall be ascribed as detailed in ANNEX I: Assets.

6. Commercial Setting for the Use of Assets owned by the other Parties

Following the end of the Project, the Parties intend to engage in commercial activities towards selling or using Products.

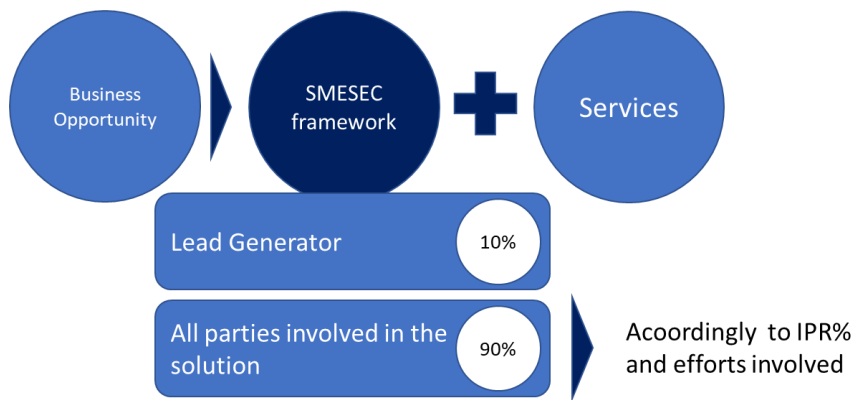
a. Definition of Asset Business Model and Price List

The Product will be offered under the SMESEC License.

The Contractor Party gets 10% of the value of the SMESEC License contract. The remaining 90% will be distributed according to the ownership and effort sharing defined in Annex II: Percentages

Additionally, the parties are entitled to offer a set of another service, including but not limited to the services of:

- Maintenance
- Consultancy
- Training



b. Roles and responsibilities

The list of roles is described below as defined in chapter 1 (Definition) but included here for convenience:

- **Lead Generator:** A Party that identifies possible Lead, starts Business Opportunity and intends to exploit Product or Assets jointly under this Agreement.
- **Contractor:** is the Party that carries out activities related to the preparation of commercial offering based on the Product, including the preparation of business opportunity dossier and actually signs contract with the customer and takes responsibility of revenue sharing as agreed in this agreement.

Nothing in this Agreement limits the Party to exploit independently and out of this Agreement any of its own Intellectual property Rights related to the Assets or to exploit independently and out of this Agreement other solutions/products present in the market and in competition with Assets.

The **Contractor Party** shall identify relevant Business Opportunities (BO) and will inform Asset IP owners, including a detailed dossier (the BO Dossier) with:

- an estimation of BO Value (defined below in this section),
- financial projections and assumptions (which for the avoidance of doubt shall be based on indicative price list proposed by the Parties in the ANNEX III: Service Description and Price list of this Agreement and the license terms and conditions of the SMESEC platform),

- together with a description of the activities in which the involvement of the other Parties could be necessary (such as professional services or similar activities with financial conditions at which such involvement is expected by the Lead Generator).

The “**BO Dossier**” should therefore also identify list of services related to Business Opportunity and Assets (such as installation, deployment, configuration, consulting, training, maintenance, support etc). If IP owners listed their indicative price for specific expert or technical services such as training, deployment, maintenance etc (price in euros per man/day) they can also have the role of Service Provider and can be included by the Contract Party in BO Dossier.

Separated Implementation arrangements can be negotiated between the Contract Party and Service Providers, including the amount of service fee, independently from IP ownership or licencing fee.

In case one or several Parties shall be involved in a Business Opportunity, they shall, together with the Lead Generator (and any third party, if need be), enter into Implementation arrangements to implement the concerned Business Opportunity. These Implementation arrangements might include purchase orders, contracts or special agreements between Concerned Parties. For the reason of transparency these arrangements should be available on request to the Concerned Parties.

The **BO Value** is the **SMESEC Licence price and sum of prices of all additional professional services or external products included in the BO**, (to be negotiated directly with the Concerned Parties based on indicative price list), but it refers the value before taxes.

Any Business Opportunity shall be presented by the Contractor Party to Concerned Parties and should be reviewed and discussed among them.

Before the celebration of the Business Opportunity agreement, the Concerned Parties:

- May, if the Contractor Party agrees to, modify the conditions of the BO Dossier (the “Modified BO Dossier”);
- Shall benefit from a right of refusal to participate to the Business Opportunity at the conditions presented in the BO Dossier or as agreed in the Modified BO Dossier, as the case may be, during the first presentation of the BO only (hereinafter referred as First Refusal).

In the case Concerned Parties accept the business conditions defined in the BO dossier, then the Lead Generator will release a **Final Approved BO Dossier**.

Nothing in this Agreement shall be understood as an obligation of the Parties to participate in any Business Opportunity or to somehow contribute in it, except expressly agreed under any written Agreement.

Each Party obligates itself vis-à-vis each and every other Party to use reasonable endeavours to perform and fulfil, promptly, actively and on time, all of its obligations under this Agreement.

Each Party hereby undertakes to use reasonable endeavours to supply promptly to the parties involved in BO all such information or documents as the party may need to carry out its responsibilities.

Each Party shall ensure the accuracy of any information or materials it supplies for the purpose of commercial activities and promptly to correct any error therein of which it is notified. The

recipient Party shall be entirely responsible for the use that such information and materials are given.

In addition, any Party hereby agrees to make available (under the conditions defined in the Implementing Arrangements) any of its assets (including, but not limited to, any right it may have on Background or the results) which is needed for use for the purpose of carrying out a Business Opportunity with other Parties.

The Parties undertake to respect and implement any standard of use of the Assets, in particular in the marketing of the Products.

Each Party has the right to carry out all the Business Opportunities in any part of the world, but in any event within, if any, the geographical scope agreed in the corresponding Implementation Arrangements.

Each Party can delegate or sub-contract to other persons the performance of a Business Opportunity, as further specified in the Implementation Arrangements.

c. Revenue sharing framework

The revenue distribution scheme to be determined for each Business Opportunity shall recognise for each Concerned Party:

- i. sales efforts, and therefore the related commission for such investments;
- ii. the value of the IPRs made available by a Concerned Party for the concerned business opportunity;
- iii. the service provision costs / investments:

It is specified that the values assigned to these items with respect to one Party in the Implementation Arrangements (e.g. contracts or specific agreements) regarding one Business Opportunity, shall also, unless otherwise agreed by the Concerned Parties, be applicable for any further Business Opportunity for which such Party participates.

Unless otherwise negotiated and agreed in the Implementation Arrangements,

- i. Only in the case of a Commercial Business Opportunity a percentage of ten (10%) of the total value of the Revenue will be paid to the Party(ies) who has(ve) generated the Business Opportunity (the Lead Generator), and
- ii. the remaining (90%) Revenue generated by the same Business Opportunity will be distributed among the Parties that participate in the Business Opportunity (Asset IP owners and Service Providers) depending on the selected business model and according to the list of Assets and Services outlined in the Final Approved BO dossier. This distribution will be negotiated for each Business Opportunity in the Implementation Arrangements and might refer to fixed amounts (e.g. licence fee, expert man-day fee) and variable amounts (e.g. pay per use) in relation to the value initially reported by BO dossier.

If, during the exploitation period of a specific Business Opportunity, there is a change in the operation or exploitation which causes a participating Party to receive a level of income which is no longer in line with the income taken into account in the Implementation Arrangements, all Concerned Parties shall agree in good faith to any modification or adaptation necessary to allow the Concerned Party to continue participating in the Business Opportunity on the same basis as originally contemplated in the initial Implementation Arrangements, except as otherwise agreed as between the Concerned Parties.

7. Liability

The Parties agree between them, for the duration of the Agreement to the following:

a. Limitations of Contractual Liability

Each Party shall indemnify each of the other Parties in respect of the acts or omissions of itself, its employees, agents and sub-contractors, resulting from the performance by it of its obligations under this Exploitation Agreement, provided always that no Party shall be responsible to any other Party for any indirect or consequential loss or similar damage such as, but not limited to, loss of profit, loss of revenue or loss of contracts, provided such damage was not caused by a wilful act.

A Party's aggregate liability for direct damages towards the other Parties collectively shall be limited to once the Party's share in the amount of incomes generated under this Agreement and actually perceived by that Party during the year preceding the date on which the damage occurs. The exclusions and limitations of liability stated above shall not apply in the case of damage caused by a wilful act.

b. Liability vis-à-vis Third Parties

Each Party shall be solely liable for any loss, damage or injury to third parties resulting from its own performance of its obligations under this Agreement.

Each Party shall remain fully responsible for the performance of any part of its obligations under this Agreement, in respect of which it enters into any contract with a third party (e.g. a subcontractor) and shall ensure such contracts enable fulfilment of this Agreement.

c. Force Majeure

No Party shall be considered to be in breach of its obligations under this Agreement if such breach is caused by Force Majeure. The Commercial Partners shall discuss in good faith about the possibilities of a transfer of rights and obligations affected by the event. Such discussions shall commence as soon as reasonably possible. If such Force Majeure event is not overcome within 6 weeks after such discussion, any affected Party shall have the right to terminate this Agreement.

8. Confidentiality

All information in whatever form or mode of communication, which is disclosed by a Party (the "**Disclosing Party**") to any other Party (the "**Recipient**") in connection with the Project and this Agreement and which has been explicitly marked as "confidential" at the time of disclosure, or when disclosed orally has been identified as confidential at the time of disclosure and has been confirmed and designated in writing within 15 calendar days from oral disclosure at the latest as confidential information by the Disclosing Party, is "**Confidential Information**".

The Recipients hereby undertake, for a period of 2 years after the end of the Agreement:

- not to use Confidential Information otherwise than for the purpose for which it was disclosed;
- not to disclose Confidential Information to any third party without the prior written consent by the Disclosing Party;
- to ensure that internal distribution of Confidential Information by a Recipient shall take place on a strict need-to-know basis;
- to apply the same degree of care with regard to the Confidential Information disclosed as with its own confidential and/or proprietary information, but in no case less than reasonable care; and
- to return to the Disclosing Party on demand all Confidential Information which has been supplied to or acquired by the Recipients including all copies thereof and to delete as far as reasonably possible all information stored in a machine-readable form. The Recipients

may keep a copy to the extent it is required to keep, archive or store such Confidential Information because of compliance with applicable laws and regulations or for the proof of on-going obligations.

The Recipients shall be responsible for the fulfilment of the above obligations on the part of their employees or third parties involved in the Project and shall ensure that they remain so obliged, as far as legally possible, during and after the end of the Project and/or after the termination of the contractual relationship with the employee or third party.

The above shall not apply for disclosure or use of Confidential Information, if and in so far as the Recipient can show that:

- the Confidential Information becomes publicly available by means other than a breach of the Recipient's confidentiality obligations;
- the Disclosing Party subsequently informs the Recipient that the Confidential Information is no longer confidential;
- the Confidential Information is communicated to the Recipient without any obligation of confidence by a third party who is to the best knowledge of the Recipient in lawful possession thereof and under no obligation of confidence to the Disclosing Party;
- the Confidential Information, at any time, was developed by the Recipient completely independently of any such disclosure by the Disclosing Party;
- the Confidential Information was already known to the Recipient prior to disclosure; or
- the Recipient is required to disclose the Confidential Information in order to comply with applicable laws or regulations or with a court or administrative order, provided that if any Party becomes aware that it will be required, or is likely to be required, to disclose Confidential Information in order to comply with applicable laws or regulations or with a court or administrative order, it shall, to the extent it is lawfully able to do so, prior to any such disclosure
 - notify the Disclosing Party when it is legally possible, and
 - comply with the Disclosing Party's reasonable instructions to protect the confidentiality of the information.

Each Party shall promptly advise the other Party in writing of any unauthorised disclosure, misappropriation or misuse of Confidential Information after it becomes aware of such unauthorised disclosure, misappropriation or misuse.

9. Termination

a. Expiration

Unless earlier terminated in accordance with the provisions of section 9.2 this Agreement shall expire in accordance with the provisions of section 3.

b. Early Termination

i. Material breach by one Party of its obligations

In case such Party would commit a material breach of its obligations hereunder, any other Party shall have the right to send to the breaching Party a notice (copying all other Parties) detailing the basis on which it believes that such Party has committed a breach and requiring that the breach be cured during a period of 20 days starting from the date on which the breaching Party receives the notice.

In case the breach would not be remedied by the breaching Party during the 20-day period referred to in the preceding paragraph, the participation of the breaching Party shall be deemed

terminated on the day falling immediately after the expiry date of the 20-day period, subject to the survival of certain clauses as provided hereunder.

ii. Termination by one Party of its participation after the Final Date

As stated in clause 3 above, each Party is entitled to terminate its participation, after the Final Date, at any moment by sending to the other Parties a termination notice in this respect, which shall take effect at least sixty (60) days after the date of the termination notice.

c. Survival of Rights and Obligations

The termination of this Agreement shall not entail the termination of any other agreement entered into in connection with this Agreement by the Parties, in particular regarding their commercial activities related to the Products.

In case of termination of this Agreement as provided in sections in sections 9.1 and 9.2 above, provisions relating to Confidentiality, commercial exploitation of the Products for the time period such exploitation is still carried out by Parties, as well as for Liability, Applicable law and Settlement of disputes shall survive the expiration or termination of this Agreement.

10. General clauses

a. No Representation, Partnership or Agency

7.2.1.1 The Parties shall not be entitled to act or to make legally binding declarations on behalf of any other Party. Nothing in this Agreement shall be deemed to constitute a joint venture, agency, partnership, interest grouping or any other kind of formal business grouping or entity between the Parties.

b. Notices and Other Communication

7.2.1.2 Any notice to be given under this Agreement shall be in writing to the addresses referred to above, unless otherwise notified to all other Parties by the Party which contact details have changed.

i. Formal Notices:

7.2.1.3 If it is required in this Agreement that a formal notice, consent or approval shall be given, such notice shall be signed by an authorised representative of a Party and shall either be served personally or sent by mail with recorded delivery or telefax with receipt acknowledgement.

ii. Other Communication:

Other communication between the Parties may also be effected by other means such as e-mail with acknowledgement of receipt, which fulfils the conditions of written form.

c. Assignment and Amendments

7.2.1.4 No rights or obligations of the Parties arising from this Agreement may be assigned or transferred by one Party, in whole or in part, to any third party without the other Parties' prior formal approval.

7.2.1.5 Amendments and modifications to the text of this Agreement require a separate agreement between all Parties, to be signed by their authorised representatives.

d. Mandatory national law

7.2.1.6 Nothing in this Agreement shall be deemed to require a Party to breach any mandatory statutory law under which the Party is operating.

e. Language

7.2.1.7 This Agreement is drawn up in English, which language shall govern all documents, notices, meetings, arbitral proceedings, if any, and processes relative thereto.

f. Applicable Law

7.2.1.8 This Agreement shall be construed in accordance with and governed by the laws of Belgium.

g. Settlement of Disputes

7.2.1.9 Should a dispute arise between the Parties concerning the validity, the interpretation and/or the implementation of this Agreement, they will solve it through mediation, according to the rules of Mediation, Brussels. The Procedure shall entail a minimum of three meetings.

7.2.1.10 The Procedure shall not be mandatory if and when its application may generate an irreparable prejudice to a party, such as in case of insolvency, non-payment of the other party or situation whereas urgency procedures are needed.

7.2.1.11 Should the mediation fail to bring about a full agreement between the parties putting an end to the dispute within 60 days of the commencement of the mediation, it shall be brought to the sole competent courts, which will be the courts of Brussels.

7.3 Annex III SMESEC- Letter of intent

SMSEC- Letter of intent relating to continued support of the SMSEC results after the project

SMESEC- Letter of intent relating to continued support of the SMESEC results after the project termination

Undertaken by:

Herein validly represented by **Sotiris IOANNIDIS** in his role as Principle Investigator for the **Foundation for Research and Technology - Hellas (FORTH)**, established in Plastira str., Vassilika Vouton, Heraklion, Crete GR Postal Code: 700 13, Greece, VAT no: GR090101655, hereafter the ‘Party’,

Having regard to the following:

- The Party participated as a partner in the SMESEC project (hereafter ‘SMESEC’, a project that has received funding from the European Union’s Horizon 2020 research and innovation programme under Grant Agreement No. 740787, to which the Party was a signatory;
- In the opinion of the Party, SMESEC has successfully produced various project outcomes which have clear market and business potential, and which can be further promoted / developed / exploited beyond SMESEC’s date of termination as set out in accordance with the Grant Agreement;
- Based on this opinion, the Party is willing and intends to provide further support as described in this Letter of Intent to the promotion, development and exploitation of SMESEC outcomes.

Therefore, the Party declares as follows:

Intent of the Party

- The Party shall make available commercially reasonable resources, in accordance with SMESEC’s market and business potential as assessed by the Party, in order to support the promotion, development and exploitation of SMESEC outcomes, notably by:
 - o *Provide all the assets, training material developed during the project’s life span under GPL licenses to all interested parties that will use SMESEC solution under contract.*
 - o *Provide installation guidance and support to the tools brought by FORTH, under bilateral contracts with specific Daily/Hourly rate.*
- The Party shall continue to engage in good faith discussions and interactions with any other SMESEC partners who have provided a comparable letter of intent, and shall work with them constructively and proactively in order to seek out and identify joint business opportunities wherever this is necessary and beneficial to the Party to realise SMESEC’s market and business potential.

For the avoidance of doubt, this Letter of Intent is limited to what is stated explicitly herein. This Letter of Intent does not create any legal undertaking, consortium, formal partnership or joint venture, nor does it result in any agency or grant any power of representation to any party. This Letter of Intent does not give rise to any transfers of property rights (including intellectual property rights), nor to any grants of licences or permissions, and it does not replace or affect in any way any legal agreements to which the Party is a signatory. This Letter of Intent does not grant any exclusivity rights and does not constitute an obligation to ensure the involvement of

Document name:	D5.5 Open Call Design, Implementation and Results Report			Page:	14 of 110
Reference:	D5.5	Dissemination:	PU	Version:	1.0
				Status:	FINAL

other parties before acting on any business or market opportunity in relation to SMESEC.

Duration and validity of this Letter of Intent

The Party shall make adequate resources available in order to make good on its intent as described above after the date of termination of SMESEC, and it shall act in accordance with this Letter of Intent, for a period of time which it deems to be useful in order to conclusively determine SMESEC's market and business potential to its own satisfaction.

The Party can freely finish this Letter of Intent fifteen (15) days after the sending of a formal notification to the other SMESEC partners who have provided a comparable letter of intent.

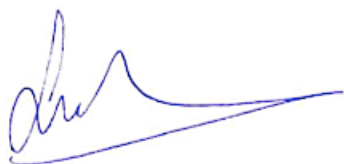
Without formal commitment on this exact duration, the Party's best efforts estimation of this period of time is presently a period of 1 years after the signing of this Letter of Intent.

This letter of intent is a good faith statement of commitment on the Party, but does not give rise to a binding legal obligation in the absence of further agreements in relation to specific business or market opportunities.

Applicable law and disputes

This Letter of Intent, including its interpretation and legal enforceability, shall be subject to the laws of Belgium, and the competent courts shall be the Courts of Brussels

Signed on 15 May, in Heraklion, by Sotiris IOANNIDIS



Document name:	D6.4 Annual report on exploitation, dissemination and standardization			Page:	15 of 110		
Reference:	D6.4	Dissemination:	PU	Version:	1.0	Status:	Final version

SMSEC- Letter of intent relating to continued support of the SMSEC results after the project termination

Undertaken by:

GridPocket SAS, established at 300 route des Cretes, 06560 Valbonne, France, registered at No 518 639 695 RCS Grasse, hereafter the 'Party',

Herein validly represented by Mr Filip GLUSZAK, in his legal capacity as President,

Having regard to the following:

- The Party participated as a partner in the SMESEC project (hereafter 'SMESEC', a project that has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement No. 740787, to which the Party was a signatory;
- In the opinion of the Party, SMESEC has successfully produced various project outcomes which have clear market and business potential, and which can be further promoted / developed / exploited beyond SMESEC's date of termination as set out in accordance with the Grant Agreement;
- Based on this opinion, the Party is willing and intends to provide further support as described in this Letter of Intent to the promotion, development and exploitation of SMESEC outcomes.

Therefore, the Party declares as follows:

Intent of the Party

- The Party shall make available commercially reasonable resources, in accordance with SMESEC's market and business potential as assessed by the Party, in order to support the promotion, development and exploitation of SMESEC outcomes, notably by:
 - o proposing SMESEC solution along its product offering when it is commercially and technically relevant,
- The Party shall continue to engage in good faith discussions and interactions with any other SMESEC partners who have provided a comparable letter of intent, and shall work with them constructively and proactively in order to seek out and identify joint business opportunities wherever this is necessary and beneficial to the Party to realise SMESEC's market and business potential.

For the avoidance of doubt, this Letter of Intent is limited to what is stated explicitly herein. This Letter of Intent does not create any legal undertaking, consortium, formal partnership or joint venture, nor does it result in any agency or grant any power of representation to any party. This Letter of Intent does not give rise to any transfers of property rights (including intellectual property rights), nor to any grants of licences or permissions, and it does not replace or affect in any way any legal agreements to which the Party is a signatory. This Letter of Intent does not



Document name:	D6.4 Annual report on exploitation, dissemination and standardization			Page:	10 of 110	
Reference:	D6.4	Dissemination:	PU	Version:	1.0	Status: Final version

grant any exclusivity rights and does not constitute an obligation to ensure the involvement of other parties before acting on any business or market opportunity in relation to SMESEC.

Duration and validity of this Letter of Intent

The Party shall make adequate resources available in order to make good on its intent as described above after the date of termination of SMESEC, and it shall act in accordance with this Letter of Intent, for a period of time which it deems to be useful in order to conclusively determine SMESEC's market and business potential to its own satisfaction.

Without formal commitment on this exact duration, the Party's best efforts estimation of this period of time is presently a period of 1 years after the signing of this Letter of Intent.

This letter of intent is a good faith statement of commitment on the Party, but does not give rise to a binding legal obligation in the absence of further agreements in relation to specific business or market opportunities.

Applicable law and disputes

This Letter of Intent, including its interpretation and legal enforceability, shall be subject to the laws of the country of establishment of the Party, and the competent courts shall be those of the country of establishment of the Part.

Signed on 22 May, in Valbonne, by Filip Gluszak



Filip Gluszak
President
GridPocket SAS

GRIDPOCKET
300 RT. DES CRETES
06560 SOPHIA - ANTIPOLIS
518 639 895 RCS GRASSE
S.S 70 CAPITAL 12714€

Document name:	D6.4 Annual report on exploitation, dissemination and standardization	Page:	17 of 110
Reference:	D6.4	Dissemination:	PU
		Version:	1.0
		Status:	Final version

SMESEC- Letter of intent relating to continued support of the SMESEC results after the project termination

Undertaken by:

Worldsensing SL, WS, established in Viriat 47, 10th floor, Barcelona E-08014, Spain, ES-B64902208, hereafter the ‘Party’,

Herein validly represented by Ignasi Vilajosana Guillen, in his legal capacity as Partner-Manager,

Having regard to the following:

- The Party participated as a partner in the SMESEC project (hereafter ‘SMESEC’, a project that has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement No. 740787, to which the Party was a signatory;

- In the opinion of the Party, SMESEC has successfully produced various project outcomes which have clear market and business potential, and which can be further promoted / developed / exploited beyond SMESEC’s date of termination as set out in accordance with the Grant Agreement;

- Based on this opinion, the Party is willing and intends to provide further support as described in this Letter of Intent to the promotion, development and exploitation of SMESEC outcomes.

Therefore, the Party declares as follows:

Intent of the Party

- The Party shall make available commercially reasonable resources, in accordance with SMESEC’s market and business potential as assessed by the Party, in order to support the promotion, development and exploitation of SMESEC outcomes, notably by:

- o Maintaining the “Industrial Pilot” operative in Patras (Greece) and report on the functioning on the company’s website.

- o Present the added-value of the SMESEC framework to selected customers and use reasonable efforts to attain an effective market adoption of the solution or some of its main components.

- o Keeping direct contact with the rest of project partners to respond to their needs in case they need Worldsensing’s direct support to exploit SMESEC outcomes.

Worldsensing S.L. - Viriat, 47 10th floor, 08014 Barcelona, Spain – B64902208

- The Party shall continue to engage in good faith discussions and interactions with any other SMESEC partners who have provided a comparable letter of intent, and shall work with them constructively and proactively in order to seek out and identify joint business opportunities wherever this is necessary and beneficial to the Party to realise SMESEC’s market and business potential.

For the avoidance of doubt, this Letter of Intent is limited to what is stated explicitly herein. This Letter of Intent does not create any legal undertaking, consortium, formal partnership or joint venture, nor does it result in any agency or grant any power of representation to any party. This Letter of Intent does not give rise to any transfers of property rights (including intellectual property rights), nor to any grants of licences or permissions, and it does not replace or affect in any way any legal agreements to which the

Document name:	D6.4 Annual report on exploitation, dissemination and standardization			Page:	18 of 110	
Reference:	D6.4	Dissemination:	PU	Version:	1.0	Status: Final version

Party is a signatory. This Letter of Intent does not grant any exclusivity rights and does not constitute an obligation to ensure the involvement of other parties before acting on any business or market opportunity in relation to SMESEC.

Duration and validity of this Letter of Intent

The Party shall make adequate resources available in order to make good on its intent as described above after the date of termination of SMESEC, and it shall act in accordance with this Letter of Intent, for a period of time which it deems to be useful in order to conclusively determine SMESEC's market and business potential to its own satisfaction.

Without formal commitment on this exact duration, the Party's best efforts estimation of this period of time is presently a period of 1 years after the signing of this Letter of Intent.

This letter of intent is a good faith statement of commitment on the Party, but does not give rise to a binding legal obligation in the absence of further agreements in relation to specific business or market opportunities.

Applicable law and disputes

This Letter of Intent, including its interpretation and legal enforceability, shall be subject to the laws of the country of establishment of the Party, and the competent courts shall be those of the country of establishment of the Part.

***Signed on 21st May 2020, in Barcelona, by IGNASI VILAJOSANA GUILLEN
[THIS DOCUMENT IS ELECTRONICALLY SIGNED]***



Firmado por 46361067J
IGNASI VILAJOSANA
(R:B64902208) el día
21/05/2020 con un
certificado emitido por
AC Firmaprofesional -
CUALIFICADOS

SMESEC- Letter of intent relating to continued support of the SMESEC results after the project termination

Undertaken by:

ATOS SPAIN SA (ATOS), established in CALLE DE ALBARRACIN 25, MADRID 28037, Spain, VAT number: ESA28240752, hereafter the 'Party',

Herein validly represented by [person name], in his/her legal capacity as Partner-Manager,

Having regard to the following:

- The Party participated as a partner in the SMESEC project (hereafter 'SMESEC', a project that has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement No. 740787, to which the Party was a signatory;

Document name:	D6.4 Annual report on exploitation, dissemination and standardization			Page:	19 of 110		
Reference:	D6.4	Dissemination:	PU	Version:	1.0	Status:	Final version

- In the opinion of the Party, SMESEC has successfully produced various project outcomes which have clear market and business potential, and which can be further promoted / developed / exploited beyond SMESEC's date of termination as set out in accordance with the Grant Agreement;
- Based on this opinion, the Party is willing and intends to provide further support as described in this Letter of Intent to the promotion, development and exploitation of SMESEC outcomes.

Therefore, the Party declares as follows:

Intent of the Party

- The Party shall make available commercially reasonable resources, in accordance with SMESEC's market and business potential as assessed by the Party, in order to support the promotion, development and exploitation of SMESEC outcomes, notably by:
 - o ATOS will coordinate, with the rest of the consortium partners willing to participate, any potential opportunity that may appear once the project ends.
 - o ATOS will maintained the SMESEC framework server running for a period of one year (April 2021). After that period and accordingly to the commercial expectations, it could be extended additionally.
 - o ATOS will participate in the dissemination and communication of the SMESEC results (e.g. meeting in December 2020) and also will extend the dissemination activities with SMEs associations (e.g. Planetic).
- The Party shall continue to engage in good faith discussions and interactions with any other SMESEC partners who have provided a comparable letter of intent, and shall work with them constructively and proactively in order to seek out and identify joint business opportunities wherever this is necessary and beneficial to the Party to realise SMESEC's market and business potential.

Document name:	D6.4 Annual report on exploitation, dissemination and standardization			Page:	20 of 110	
Reference:	D6.4	Dissemination:	PU	Version:	1.0	Status: Final version

For the avoidance of doubt, this Letter of Intent is limited to what is stated explicitly herein. This Letter of Intent does not create any legal undertaking, consortium, formal partnership or joint venture, nor does it result in any agency or grant any power of representation to any party. This Letter of Intent does not give rise to any transfers of property rights (including intellectual property rights), nor to any grants of licences or permissions, and it does not replace or affect in any way any legal agreements to which the Party is a signatory. This Letter of Intent does not grant any exclusivity rights and does not constitute an obligation to ensure the involvement of other parties before acting on any business or market opportunity in relation to SMESEC.

Duration and validity of this Letter of Intent

The Party shall make adequate resources available in order to make good on its intent as described above after the date of termination of SMESEC, and it shall act in accordance with this Letter of Intent, for a period of time which it deems to be useful in order to conclusively determine SMESEC’s market and business potential to its own satisfaction.

The Party can freely finish this Letter of Intent fifteen (15) days after the sending of a formal notification to the other SMESEC partners who have provided a comparable letter of intent.

Without formal commitment on this exact duration, the Party’s best efforts estimation of this period of time is presently a period of 1 years after the signing of this Letter of Intent.

This letter of intent is a good faith statement of commitment on the Party, but does not give rise to a binding legal obligation in the absence of further agreements in relation to specific business or market opportunities.

Applicable law and disputes

This Letter of Intent, including its interpretation and legal enforceability, shall be subject to the laws of Belgium, and the competent courts shall be the Courts of Brussels.

Signed on 3 June, in Madrid], by Alicia Garcia Medina

[Signature and/or company stamp]

Document name:	D6.4 Annual report on exploitation, dissemination and standardization			Page:	21 of 110	
Reference:	D6.4	Dissemination:	PU	Version:	1.0	Status: Final version