Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

SMESEC

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

# D6.1 Dissemination plan and market analysis

| **Document Identification** | | | |
|---|---|---|---|
| **Status** | Final version | **Due Date** | 30/11/2017 |
| **Version** | 2.0 | **Submission Date** | 05/12/2017 |

| | | | |
|---|---|---|---|
| **Related WP** | WP6 | **Document Reference** | D6.1 |
| **Related Deliverable(s)** | | **Dissemination Level (*)** | PU |
| **Lead Organization** | EGM | **Lead Author** | Giunta Nicolas, EGM |
| **Contributors** | FHNW<br>UU<br>ATOS | **Reviewers** | Ioannidis Sotiris, FORTH<br>Lampropoulos Kostas, UoP |

**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.

# Document Information

| List of Contributors | |
|---|---|
| Name | Partner |
| Cousin Philippe, Giunta Nicolas | EGM |
| Fricker Samuel | FHNW |
| Spruit Marco | UU |
| Ruiz José Francisco, Miranda Garcia Alberto | ATOS |
| Oikonomou George | CITRIX |

| Document History | | | |
|---|---|---|---|
| Version | Date | Change editors | Changes |
| 0.1 | 05/10/2017 | EGM | Table of contents |
| 0.2 | 19/10/2017 | EGM | Content development, update of ToC |
| 0.3 | 19/10/2017 | FHNW | Outline Dissemination section |
| 0.4 | 26/10/2017 | EGM | Content development, details target groups definition |
| 0.5 | 27/10/2017 | FHNW | Complete draft dissemination section |
| 0.6 | 30/10/2017 | EGM | Dissemination integration - restructuring |
| 0.7 | 30/10/2017 | ATOS | First draft market analysis section |
| 0.8 | 02/11/2017 | UU | Complete draft standardisation section |
| 0.9 | 06/11/2017 | EGM | Rewriting – Complete full draft version |
| 1.0 | 13/11/2017 | | FINAL FIRST DRAFT VERSION |
| 1.1 | 14/11/2017 | CITRIX | WP2 coordination on market analysis |
| 1.2 | 14/11/2017 | ATOS | Update and content integration |
| 1.3 | 14/11/2017 | FHNW | Update in dissemination messages |
| 1.4 | 14/11/2017 | EGM | FINAL DRAFT – VERSION FOR REVIEW 1 |
| 1.5 | 22/11/2017 | FHNW | Update of dissemination based on review comments |
| 1.6 | 28/11/2017 | ATOS | Update in conclusions |
| 1.7 | 28/11/2017 | EGM | FINAL DRAFT – VERSION FOR REVIEW 2 |
| 1.8 | 30/11/2017 | ATOS | Update and minor corrections from review 2 |
| 1.9 | 01/12/2017 | EGM | FINAL VERSION |
| 2.0 | 05/12/2017 | ATOS | Quality control and submission |

# Table of Contents

# List of Tables

# List of Figures

# 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 |

| Abbreviation / acronym | Description |
|---|---|
| ISO | International Organization for Standardization |
| IT | Information Technology |
| IPR | Intellectual Property Right |
| JVM | Java Virtual Machine |
| KPI | Key Performance Indicators |
| 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 |

# Executive Summary

In order to maximise the impact of its results, SMESEC will implement a strategy based on a multi-dimensional approach to foster dissemination, exploitation and standardisation activities. As a market-driven project, and due to the scope of the project, it will especially focus on SMEs, delivering a dedicated cybersecurity framework. To ensure the wider audience, SMESEC will lead direct communication activities, among others, towards companies in order to generate awareness in top management, decisions makers, foster the framework adoption by technicians and developers by organising workshops/trainings, enhancement of products and services, and open-source software contributions.

Acting as a driver of cybersecurity market, these SMEs' oriented activities will be strengthened by a set of scientific and informational publications, associated with standardisation contributions in order to consolidate international and European links and harmonizing solutions with general standards and directives – promoting cybersecurity policies and models. This active participation will give relevancy, added solidity and open other new networks of SMEs involved in the satellite fields of cybersecurity.

As SMESEC aims at delivering an advanced cybersecurity framework for SMEs, its concept is broad enough to address a wide range of fields of application. To optimise its effectiveness and massive adoption, it is planned to firstly focus on the four project's pilot use cases (IoT, Smart City, Smart Grid, eVoting), build vertical communities and extend them in a second time to a broader range of industrial domains through an open call system.

The dissemination activities will be supported by a set of communication actions meeting the SMESEC objectives and notably in:

- Ensuring project visibility by generalised marketing of the project activities via selected media and dissemination channels.
- Fostering the SMESEC Framework adoption via targeted marketing of specific activities and outcomes to identified target groups.
- Supporting a sustainable exploitation of the SMESEC outcomes.
- Contributing in policy and standards related activities.

This deliverable presents the preliminary dissemination and standardization plans taking into account the project assets and their current status. Market links will be maintained all along the project lifetime and each plan will be continuously updated to match expectations and stakeholders needs, supporting the future exploitation plan.

# 1 Introduction

## 1.1 Purpose of the document

This document presents the preliminary market analysis and the corresponding dissemination and standardization plan that will be developed during the SMESEC project. The initial plan provides an overview of the communication and standardization strategy, presenting the materials, the channels, and the target groups of the project. This strategy will be updated and adjusted all along the full duration of the project to maximize the project's impact and will be completed with the exploitation plan presented in the next deliverable.

## 1.2 Relation to other project work

As a preliminary plan, this deliverable defines concrete actions derived from the description of action, defining distinct phases and respective roles of SMESEC partners. This work is also based on all WPs and especially on WP2 bringing inputs for technical understanding and use cases definition. This pushed a complementary approach to the current market analysis.

## 1.3 Structure of the document

This document is structured in four major chapters

**Chapter 1** presents the SMESEC assets and relative IPRs.

**Chapter 2** presents a market analysis presenting possible competitors and market maturity for each project asset.

**Chapter 3** presents the preliminary dissemination plan, including strategy, materials and schedule of activities.

**Chapter 4** presents the standardization strategy plan, depicting general strategy and associated partners' actions.

# 2 Project assets

## 2.1 Project assets

### 2.1.1 SMESEC Framework as a unified solution

The SMESEC project aims to deliver a complete framework able to provide validated solutions to secure SMEs. This section presents some outputs from WP2 trying to give an overview of main technological features and their impacts on a reference architecture (shown in Figure 1).

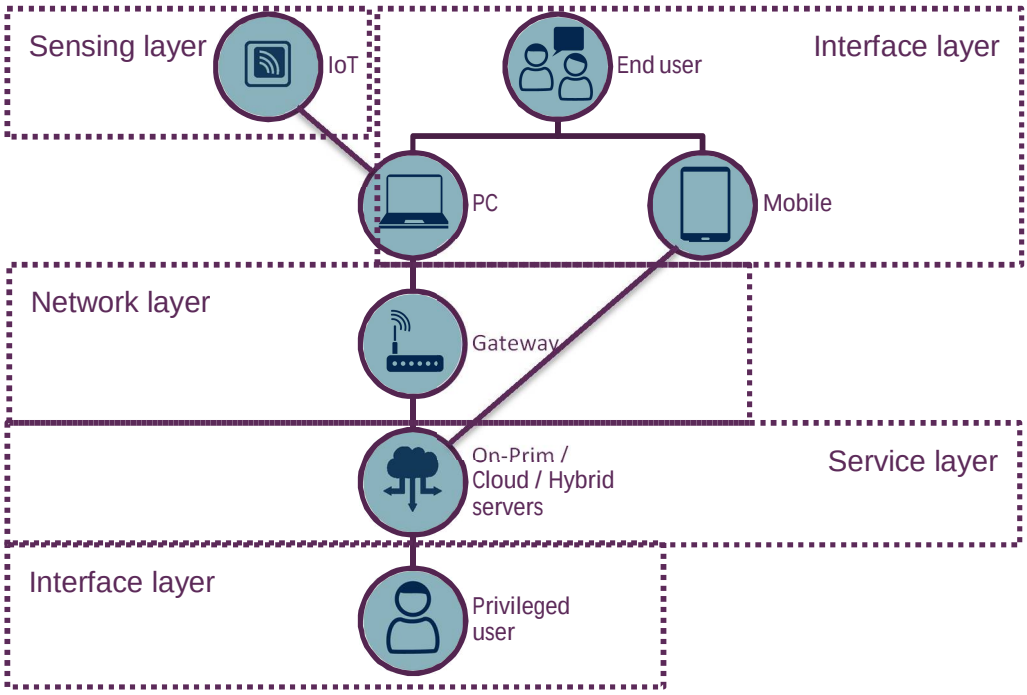


**Figure 1: SMESEC reference architecture and different system layers**

The table below depicts the main technologies addressed in the SMESEC project and their impacts on the different layers of IT systems.

| **Security products \ System layers** | **Sensing layer** | **Network layer** | **Service layer** | | | **Application / Interface layer** |
|---|---|---|---|---|---|---|
| Security products \ Data chain function | Data collection | Data carriage | Data storage | Data analytics | Data market place | Data use |
| Encryption | ✔ | ✔ | ✔ | | | |
| Governance, Risk, Compliance | | | ✔ | ✔ | ✔ | ✔ |

| Security products \ System layers | Sensing layer | Network layer | Service layer | | | Application / Interface layer |
|---|---|---|---|---|---|---|
| Data Loss Prevention | ✔ | ✔ | ✔ | | | ✔ |
| Unified Threat Management | ✔ | ✔ | ✔ | ✔ | | ✔ |
| Security Information and Event Management | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ |
| Intrusion Detection and Prevention Systems (IDS/IPS) | ✔ | ✔ | | ✔ | ✔ | ✔ |
| Distributed Denial-of-Service Mitigation | | ✔ | ✔ | ✔ | | |
| Business Continuity / Disaster Recovery | ✔ | ✔ | ✔ | | ✔ | ✔ |
| Web Application Firewall | | ✔ | | ✔ | ✔ | |
| Secure Web Gateway | | ✔ | | ✔ | ✔ | ✔ |
| Application Security Testing (AST) | ✔ | | ✔ | | ✔ | ✔ |
| Endpoint protection platform (EPP) | ✔ | ✔ | ✔ | | ✔ | ✔ |
| Security Awareness and Training | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ |
| Deception technology | | ✔ | ✔ | | | ✔ |
| Endpoint Detection and Response (EDR) | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ |
| Cloud Access Security Brokers (CASB) | | ✔ | | ✔ | | ✔ |
| User Entity Behaviour Analytics (UEBA) | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ |
| Identity & access management | | ✔ | ✔ | ✔ | | ✔ |

**Table 1: SMESEC framework technologies and layers impacts**

### 2.1.2 SMESEC Framework components

#### 2.1.2.1 Encryption

Encryption refers to the process of protecting sensitive data by converting it to an encoded form that can only be decrypted by means of a protected key. This method ensures that even if security is breached in other levels, data will still be highly protected and will be useless to any malicious user.

#### 2.1.2.1 Governance, Risk Management and Compliance (GRC)

Governance, Risk Management and Compliance (GRC) is a term often used to describe the organization's efficiency to achieve its objectives, address uncertainty and act with integrity. In these three terms, (i) Governance refers to the processes involved to assure that the organization handles information properly across all workflows, (ii) Risk Management stands for predicting and handling possible risks that may slow the organization achieving the goals and (iii) Compliance includes all the processes to adhere with laws and regulations, as well as company policies (such as PCI DSS, HIPAA, HITRUST, EI3PA, SOX, GLBA, FISMA, ISO 27001).

#### 2.1.2.2 Data Loss Prevention

Data loss prevention is the set of security controls for protecting sensitive enterprise data from being disclosed to unauthorized users, across all platforms (computers, mobile, etc.) and throughout its life cycle.

#### 2.1.2.3 Unified Threat Management (UTM)

Unified Threat Management is the all-in-one security solution that integrates multiple solutions, such as antivirus, VPN, firewalls, content filtering, etc. often running simultaneously.

#### 2.1.2.4 Security Information and Event Management (SIEM)

Security Information and Event Management (SIEM) is a technology that enables the aggregation of data produced by multiple devices, network infrastructure, systems, and applications. Log data may be the primary source of information but SIEM systems are able to consume more complex data structures. Combined with other sources, such as user directories, vulnerabilities, etc. SIEM systems are able to monitor systems and users as well as compliance to policies and standards.

#### 2.1.2.5 Intrusion Detection and Prevention System (IDS/IPS)

Intrusion Detection/Prevention Systems implement threat deterrent technologies that monitor live network traffic to detect and prevent vulnerabilities based on a given set of rules.

#### 2.1.2.6 Distributed Denial-of-Service mitigation (DDoS)

Distributed Denial-of-Service (DDoS) refers to the type of attacks from multiple sources to a single target that causes denial of service due to flooding by immense traffic. It directly affects the organization operations by denying access to legitimate users.

#### 2.1.2.7 Business Continuity / Disaster Recovery

Business Continuity Management plans the crisis management processes though a configurable system to describe the business continuity needs, analyse the risks, create and test business continuity plans and initiate and manage the disaster recovery activities.

#### 2.1.2.8 Web Application Firewall (WAF)

Web Application Firewall differ from the typical firewall as they focus mainly on protecting the web traffic (HTTP protocol) from a variety of attacks, such as Cross-Site Scripting (XSS), SQL injection, etc. WAFs are able to inspect the payload of the HTTP traffic and decide if this is legit, and provide input to other tools like SIEMs.

#### 2.1.2.9 Secure Web Gateway (SWG)

Secure Web Gateways protect company assets while surfing and enforce the policy companies to the network traffic. They may offer a range of capabilities, including URL filtering, antivirus/antimalware protection, SSL traffic inspection, etc.

#### 2.1.2.10 Application Security Testing

Application Security Testing help developers, administrators, enterprises, etc. identify security vulnerabilities by performing exhausting testing on various aspects of the software. It may be also categorized as:

- Static Application Security Testing (SAST): Essentially white box testing, allows the source code to be examined for vulnerabilities.
- Dynamic Application Security Testing (DAST): Black box testing by running the software under many different environments and inputs without access to source code.
- Run-time Application Security Protection (RASP): Testing by examining the runtime environment of the application (e.g. JVM) using instrumentation.
- Interactive Application Security Testing (IAST): This is a combination of SAST and RASP, allowing users to check various attack scenarios and the effect on the runtime environment.
- Mobile Application Security Testing (Mobile AST): Combination of SAST, DAST and behavioral analysis using static and dynamic techniques to identify.

#### 2.1.2.11 Security Awareness and Training

Humans are usually the weakest point in cyber security. Either by their online behaviour (browsing malicious sites, unwittingly disclosing sensitive information, fall prey to social engineering attacks, etc.), or by bringing into the infrastructure infected devices (laptops, etc.), they impose a serious risk in the organization's security measures.

A number of companies are focusing on increasing security awareness and educating employees and users in general on security aspects and best practices for their everyday online habits.

#### 2.1.2.12 Endpoint protection platform (EPP)

An endpoint protection platform (EPP) is a solution that converges endpoint device security functionality into a single product that delivers antivirus, anti-spyware, personal firewall, application control and other styles of host intrusion prevention (for example, behavioural blocking) capabilities into a single and cohesive solution. More advanced EPP solutions are starting to integrate with vulnerability, patch and configuration management capabilities for more proactive protection. Beyond fighting malware, modern EPP products are expanding to include data protection features, such as disk and file encryption, data loss prevention, and device control. The majority of the EPP market is focused on PC-type endpoints; however, these solutions increasingly are starting to encompass management and tracking of other mobile devices, such as tablets and smartphones.

#### 2.1.2.13 Security Information and Event Management (SIEM)

Security information and event management (SIEM) technology supports threat detection and security incident response through the real-time collection and historical analysis of security events from a wide variety of event and contextual data sources. It also supports compliance reporting and incident investigation through analysis of historical data from these sources. The core capabilities of SIEM technology are a broad scope of event collection and the ability to correlate and analyse events across disparate sources.

#### 2.1.2.14 Deception technology

Deception technologies are defined by the use of deceit and/or feints designed to thwart or throw off an attacker's cognitive processes, disrupt an attacker's automation tools, delay an attacker's activities or disrupt breach progression. Deceptions are achieved through the use of deceitful responses, purposeful obfuscations, feints, misdirections and other falsehoods. These techniques leverage the trust that attackers and the attackers' tools must have in the network protocols, infrastructure, applications, systems and data elements they interact with or access during the execution of their attacks or throughout their intelligence gathering activities. Deception in this context is used as a technique for defensive or disruptive purposes, and is not offensive in nature.

#### 2.1.2.15 Endpoint Detection and Response (EDR)

Endpoint Detection and Response is the next step in Endpoint Protection Platforms (EPP). Typically, EPP involves the detection and mitigation to a more sophisticated process including detection, analytics and prioritization of incident response.

#### 2.1.2.16 Cloud Access Security Brokers (CASB)

Cloud access security brokers (CASBs) are on-premises, or cloud-based security policy enforcement points, placed between cloud service consumers and cloud service providers to combine and interject enterprise security policies as the cloud-based resources are accessed. CASBs consolidate multiple types of security policy enforcement. Example security policies include authentication, single sign-on, authorization, credential mapping, device profiling, encryption, tokenization, logging, alerting, malware detection/prevention and so on.

#### 2.1.2.17 User Entity Behaviour Analytics (UEBA)

User and entity behaviour analytics offers profiling and anomaly detection based on a range of analytics approaches, usually using a combination of basic analytics methods (e.g., rules that leverage signatures, pattern matching and simple statistics) and advanced analytics (e.g., supervised and unsupervised machine learning). Vendors use packaged analytics to evaluate the activity of users and other entities (hosts, applications, network traffic and data repositories) to discover potential incidents.

#### 2.1.2.18 Identity & access management (IAM)

Identity and access management (IAM) is the security discipline that enables the right individuals to access the right resources at the right times for the right reasons. IAM addresses the mission-critical need to ensure appropriate access to resources across increasingly heterogeneous technology environments, and to meet the advancing rigorous compliance requirements. This security practice is a crucial undertaking for any enterprise. It is fully business-aligned, and it requires business skills, not just technical expertise. Enterprises that develop mature IAM capabilities can reduce their identity management costs and, more importantly, become significantly more agile in supporting new business initiatives.

# 3 Market analysis

## 3.1 Introduction

As part of market analysis (a quantitative and qualitative assessment of a market), SMESEC project has initiated a first approach to the key drivers in order to create a basis for the design and development of the objectives of the project. SMEs represent in Europe about 99% of the total number of established companies and contribute in about 60% in the value-added production. Usually early adopters and first players in emerging markets, SMEs are facing today cybersecurity threats that may seriously hinder the company's development. Larger enterprises can afford costly security solutions and own expertise resources to prevent alert and react to cyberattacks and cybercrime threats.

In order to select appropriate channels, messages and efficiently tune the SMESEC value proposition, the focus has been placed in the current and forthcoming market domains for SMEs, the size of the market for both volume and value and the key competitor for each domain. The objectives of this task are to better understand the market to increase the SMESEC potentialities with a tri-angled approach as illustrated in the Figure 2: Overview of SMESEC market analysis approach by:

- Analyzing current trends, performing market segmentation and investigating market barriers.
- Surveying the existing technologies, potential competitors and their distinctive features. (described in D2.1)[1]
- Assessing selected business and technology transfer models in different EU countries and defining a deployment strategy for SMESEC partners.

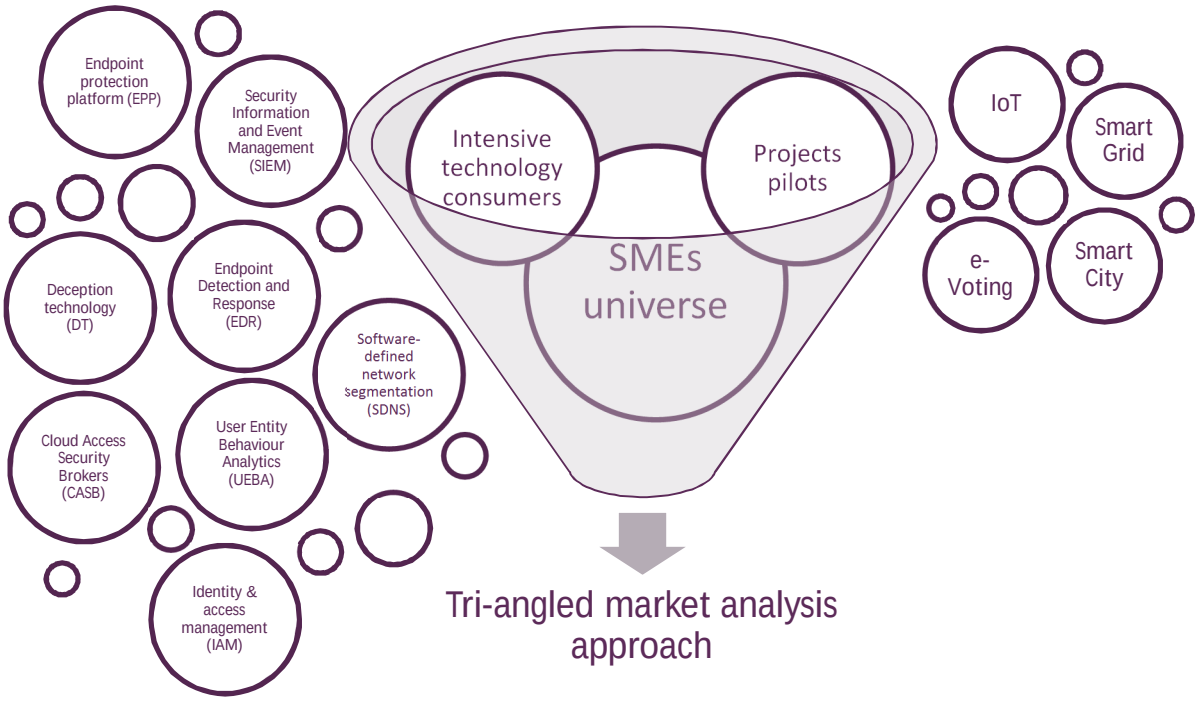


**Figure 2: Overview of SMESEC market analysis approach**

A top-down market analysis approach will include the generic SMEs' market domain up to the use case pilots' market domains alongside with new emerging markets where SMEs have a specific weight. As a living document, market will be monitored throughout the project's lifetime and any major impact on the analysis would be reported in the forthcoming exploitation documents.

## 3.2 SMESEC motivation

The problem of **cyber-security** is a complex one. Each company with its services and products has its own peculiarities and requirements forcing solutions to be tailored-made for each case individually.

Due to this, security solutions are expensive in both time and money, are highly complex and require a dedicated expert team to setup and manage. Big organizations have specific allocated budgets to pay the price to protect them as a potential breach could have severe economical and reputational impacts. SMEs and public administrations, on the other hand, have limited budgets and are generally reluctant to invest in cyber-security.

*"A survey of over 1,000 UK SMEs also showed that almost half – or 49 per cent – admitted that they plan to spend £1,000 or less on their cyber defences in the next 12 months, while 22 per cent said that they don't know how much they will spend [2]".*

Reality shows that security is not a key driver in their agendas (only 27% of small businesses have a formally defined ICT security policy [3]), focusing on generate new services and products with two main objectives: **time to market and cost minimization**.

The threats to **cyber-security have been given prominence by recent EU projects** as one of the most important emerging threats to our security.

The damage caused by cybercrimes will increase from **$3 trillion in 2015 to $6 trillion globally by 2021** as presented in Tufin infographic, 80% of the cybercriminals are affiliated with organized crime.

In June 2014 the McAfee study "Net Losses: Estimating the Global Cost of Cybercrime", depicts an estimation of the economic impact of cybercrime for the EU, as 0.41% of GDP (about 60.8 Bn euro) to be compared with 64% of GDP in USA.

Overall losses recorded in European Union: UK was the most studied country in EU, as we have identified in 3 studies. According to one study UK companies' losses reach up to 37 billion euro per year (27 billion pounds). As a comparison, this was approximately the investment of the European Commission in Innovation, Research and Development during a three-year period for the entire H2020 program. Another study underlines that the economic impact can vary between 1.01 (£544,000) to 26.19 million euro (£14 million) annual cost per company. Cost from 104,000 (£75,000) to 4.35 million euro (£3.1 million) per affected company are also mentioned. Germany is also in the focus of one of the studies with losses varying from 425,000 to 20 million euro per company per year [5] . France is also affected by losses from 445,000 to 18.9 million euro economic impact per company per year.

Securing network and information systems in the EU are essential to keep the online economy running and to ensure prosperity [4]. The following research shows this tendency [5]:

86% of the Europeans believe that the risk of becoming a victim of cybercrime is increasing. Sectors like transport, energy, health and finance have become increasingly dependent on network and information systems to run their core businesses.

Cyber incidents and attacks are on the rise:

- +4,000 ransomware attacks per day in 2016.

- In some Member States 50% of all crimes committed are cybercrimes.
- Security incidents across all industries rose by 38% in 2015 – the biggest increase in the past 12 years.
- 80% of European companies experienced at least one cybersecurity incident last year.
- +150 countries and +230,000 systems across sectors and countries were affected with a substantial impact on essential services connected to the internet, including hospitals and ambulance services.

The scale of the problem makes it necessary to act at the European level. Recent figures show that digital threats are evolving fast: ransomware attacks have increased by 300% since 2015. According to several studies, the economic impact of cybercrime rose fivefold from 2013 to 2017, and could further rise by a factor of four by 2019 whereas companies are still lacking from knowledge, awareness to protect their assets as depicted in Figure 3. Evidence suggests that people from around the world identify cyber-attacks from other countries among the leading threats to national security [6].


**Figure 3: Cybersecurity awareness [6]**

Regardless of the latent reluctance towards cybersecurity measures adoption manifested in several studies, there is a constant growing trend that shows how important are the adoption of these measures in the daily operation of SME's activities. The following paragraphs show the results of some surveys that investigate this issue [7]:

- Half of the SMEs, polled in a survey[1], have had **cyber security conditions included in contracts** with enterprise customers in the past five years.
- 33% (of the 250 IT decision-makers polled at UK) SMEs said they have had their **cyber security measures questioned as part of winning contracts** in the past year.
- 44% said they **have been required to have a recognized cyber security standard**, such as ISO 27001, by their enterprise customers in the past five years and 28% in the past year alone.
- The **threat of sanctions** by the Information Commissioner's Office (ICO), the looming deadline for compliance with the EU General Data Protection Regulation (GDPR), and fear of reputational damage from a data breach mean that **enterprises are increasingly looking at the security of their entire IT estate**, including third-party suppliers.

Other findings from the study include:

- Just over two in five (43%) organizations have cyber insurance to protect against data breaches.
- Less than half of organizations had begun taking data protection steps ahead of GDPR implementation.

[1] https://www.cybsafe.com/en-gb/enterprise-it-leaders-demanding-more-stringent-cyber-security/
http://www.computerweekly.com/news/450423617/Enterprises-are-upping-security-demands-on-SME-suppliers

- More than two in five respondents would inform all customers immediately following a data breach.
- Just over half have been asked about employee cyber security training by enterprise customers.

Figure 4 presents some uplifting statistics related to SME's cybersecurity[2]:

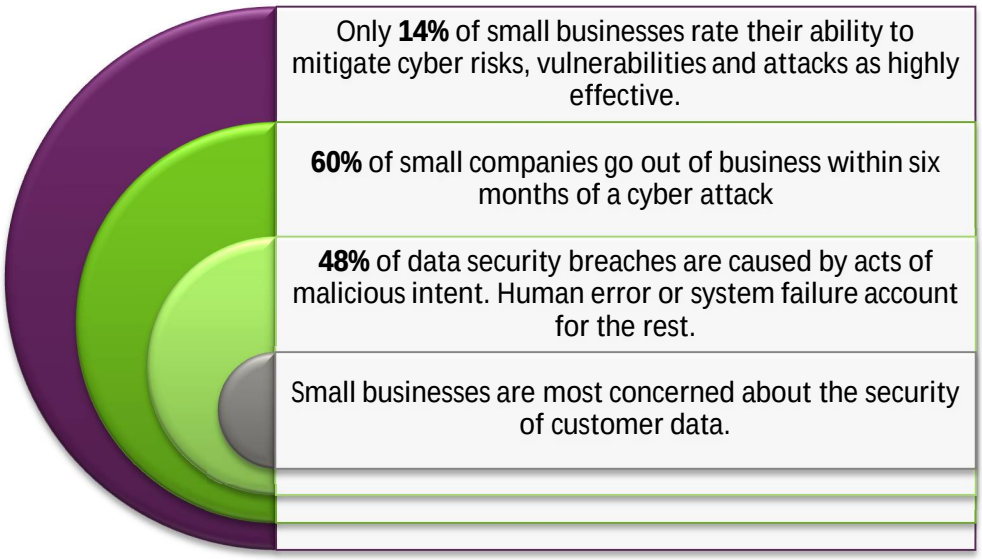


**Figure 4: SME's cybersecurity statics [8]**

From the demand point of view, SME's are receiving a massive amount of inputs from different perspectives (regulatory, customers and internal organization) which are paving their path to the cybersecurity awareness and therefore to the adoption of measures to minimise the impacts generated by the lack of the appropriate systems.

Even if cybersecurity is a common issue for citizens, governments and companies of any size, the level of awareness is not matched for the existing threats. Large companies represented in 2011 half of the documented cyberattacks, but this situation tends to change in the past years. This ratio has changed and SMEs registered 53% of total cyberattacks as shown in Figure 5. SMEs are increasing as the target for hackers because of structural and behavioural features.

[2] Small business trends (https://smallbiztrends.com/2017/01/cyber-security-statistics-small-business.html)

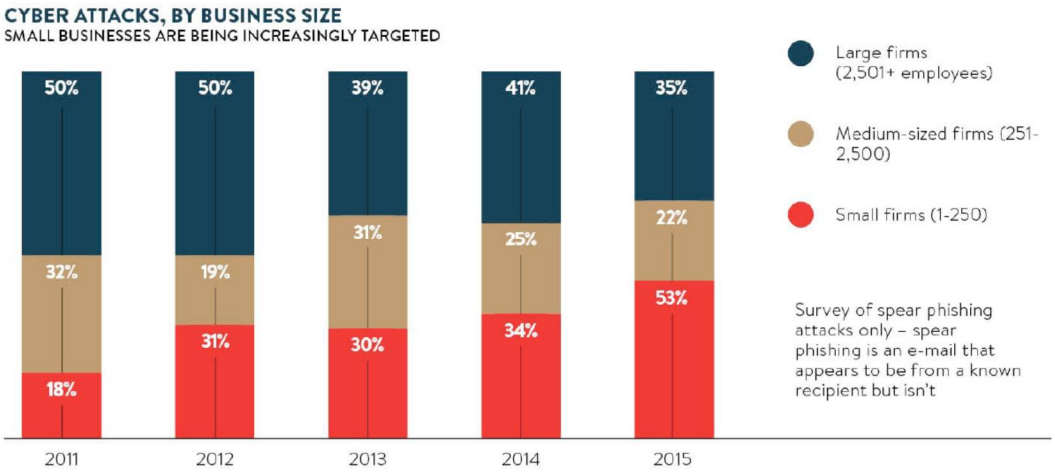


**Figure 5: Cyberattacks by business size (Symantec report 2016) [13]**

The phenomenon is such that a Zurich Insurance report on November 2016 underlined that ”a decreasing percentage of SMEs feel safe when thinking about cybercrime, with theft of customer data being the most concerning effect”. Damage reputation and business disruption are also common fears in the European SMEs. Security refers to a subjective notion but figures also confirmed the trend: A study of Barclaycard [9] shows that 48 per cent of SMEs fell victim to at least one cyber-attack in 2016 and 10 per cent were targeted multiple times.

## 3.3 Market analysis

### 3.3.1 Market trends

The following spider chart shown in Figure 6 represents both the traditional and emerging market segments of the main security product areas. An initial approach has been done in order to position SMESEC current scope in the chart, but also to see where SMESEC framework might want to be placed at the end of the project.

The red area represents the current situation and the yellow one the expected area at the end of the project. The percentage in the scale represents the coverage of the SMESEC framework for each topic visualized in the whole picture (main market segments identified).

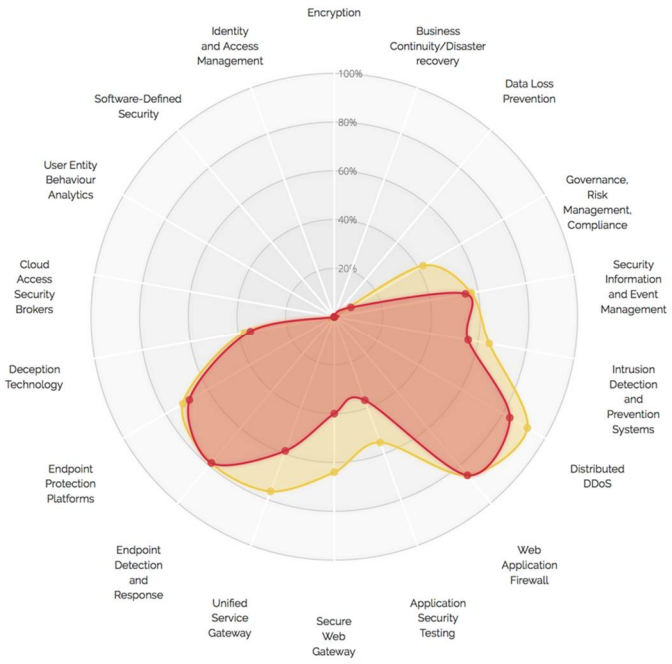


**Figure 6: Security market coverage for the SMESEC framework**

This preliminary analysis of the market shows a wide range of the market segments which will receive a direct benefit from SMESEC project's developments. Along with the technical evolution of the project, the final version of the business plan will show a well-defined impact of the SMESEC technologies and the market segments under its umbrella.

A general overview to the global cybersecurity market shows an expected size growth from **USD 137.85 Billion in 2017 to USD 231.94 Billion by 2022**, at a Compound Annual Growth Rate **(CAGR) of 11.0%** during the forecast period [10].

### 3.3.2 PEST analysis

An initial P.E.S.T analysis has been carried out around the SMESEC framework adoption (See Table 2). As result of this analysis, several Barriers and obstacles have been identified that can have a direct impact on the project's achievement (as initially mention in the Grant agreement document[3]).

The first barrier is the **traditional working method**, which still exist in many SMEs. It is not only an issue of technological support, but a socio-economical challenge. Such barrier can be smoothened with a number of measures mentioned below that will be supported through the SMESEC results.

[3] Grant Agreement number: 740787 — SMESEC — H2020-DS-2016-2017/H2020-DS-SC7-2016

**Table 2 : P.E.S.T Analysis of SMESEC framework**

| Variable | Description |
|---|---|
| **Political/Regulatory** | New requirements through regulations could have an impact on the technical solutions developed in the SMESEC project e.g. EU policies for privacy, data protection (as direct impacts on the materialization of benefits for industrial partners). There are no known regulations or standards at this time that restrict/limit or prohibit the use of the proposed technology in Europe. |
| **Economical/Business & Market:** | SMESEC puts a considerable emphasis on all inputs to be collected from businesses and markets in order to orient the implementation. This will drive the project to focus the implementation into the more important requirements which represent the specific market's needs. Since security solutions are most of the time seen as an added cost without providing new business opportunities, SMESEC will study this barrier in two levels:<br>• Costs for the provided security products/services.<br>• Provide necessary examples and proofs of the negative economic impacts that potential cyber-attacks have on businesses. |
| **Societal** | Reluctance to new technology acceptance (from awareness to economic concerns) would have a significant impact on SMESEC adoption. On the other hand, concerns on security, specifically in terms of access to sensitive information, may represent an important obstacle for proper adoption of SMESEC solutions. Since security is not only a technological issue, but also involves several organizational and procedural issues, SMESEC also plans to provide security guidelines addressing this purpose. The collaborative approach proposed by SMESEC naturally faces one of the most basic pre-conditions for any collaborative work: the **trust building.** Another societal barrier is human understanding of what SMESEC is building, and how to ensure this project has a common understanding, especially given the number of disciplines involved. |
| **Technological** | SMESEC pays extreme attention to the interoperation of all kind of modules playing a role within the cyber-security environment. Support of existing and proposed standards is mandatory in order to guarantee the full integration and features of all relevant components and interaction with external systems. Non-adoption of these standards would frustrate or prevent connections to some devices or external software and systems, or loss of features, thus impacting business potential and revenue. Following, we summarize technological barrier in a list of important issues:<br>1-**Replicability of proposed solutions for different domains:** SMESEC solutions will be tested in the pilot activities but also in the exploitation activities that will engage potential early adopters and stakeholders across Europe as soon as possible (moving from pilot solutions to additional local/regional testing-SMESEC has an open call in scope to extend the framework adoption).<br>2-**Complexity for the technicians:** The proposed solutions will have to be managed by technician staffs of generic SMEs, which are not security experts. SMESEC will define user-friendly tools in order to facilitate their use and understanding.<br>**3-Interoperability and standard solutions**: SMESEC will cope with a large diversity of components / subsystems developed using different technologies; the adoption of interoperable mechanisms is expected to lower this obstacle, which nevertheless cannot be underestimated. |

### 3.3.3 Market segmentation

**Market segmentation** *"is the process of dividing a broad consumer or business market, normally consisting of existing and potential customers, into sub-groups (segments) based on some type of common characteristics, needs, interests, etc"[11].*

Regardless of the marketing theory (to identify *high yield segments* – segments that are likely to be the most profitable or that have growth potential), SMESEC aims to become a "ready to market solution with an immediate market impact. With international and European links, the project will provide a harmonized solution with high quality and affordable cybersecurity tools validated in multiple SMEs environment. Increasing SMEs protection will also be ensured by focusing on increasing awareness and training among these organizations.

SMESEC approach to the market segmentation comes from a tri-angled perspective. Key driver of the SMESEC project orbits around **SME's in Europe** (primary target), therefore the direct market target should include all SME's (In 2015, just under **23 million** SMEs generated **€3.9 trillion in value added** and **employed 90 million people** as illustrated in Figure 7) [12].

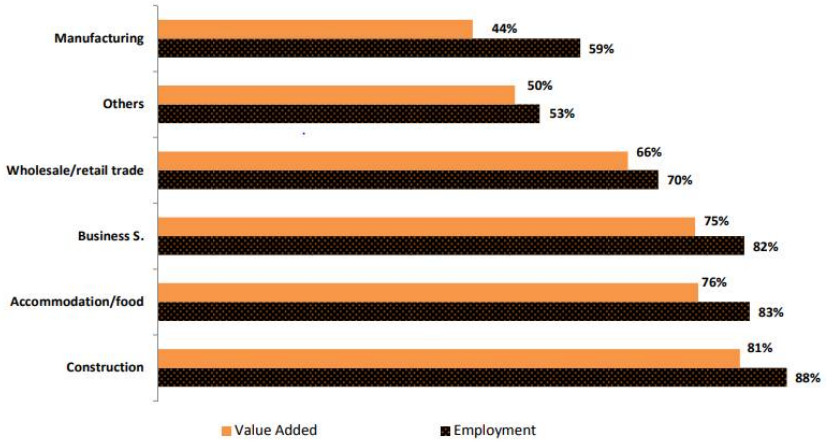


**Figure 7: Europe's SMEs by sector [12]**

A more specific target (secondary target) will place the focus on the main SME's areas where cybersecurity developments can generate a greater added value to the organization which implements those enhancements:

- Data management

According to the "**Europe IoT Data Management Market Report (2017 – 2023)**" [14], published by KBV research, the Europe Internet of Things (IoT) Data Management SMEs Market would witness market growth of 16.1% CAGR during the forecast period (2017 – 2023). Other studies [15] value globally this market in **USD 23.8 Billion in 2016 and are projected to reach USD 66.44 Billion by 2022**, at a Compound Annual Growth Rate (CAGR) of 19.3%.

The Germany market holds the largest market share in Europe Small & Medium Enterprises IoT Data Management Market by Country in 2016, and would continue to be a dominant market till 2023; growing at a CAGR of 18.8 % during the forecast period.

The Smart Manufacturing market holds the largest market share in Europe IoT Data Management Market by Application in 2016, and would continue to be a dominant market till 2023; growing at a CAGR of 14.8 % during the forecast period. The Smart Healthcare market is expected to witness a

CAGR of 15.6% during (2017 –2023). Additionally, The Connected Logistics market is expected to witness highest CAGR of 19.6% during (2017 – 2023).Source: KBV Research Analysis.

Finally, an indirect approach to the market segmentation with a fine-grained domain selection can specifically target the main beneficiaries of SMESEC development. This approach can be done from both vertical and horizontal perspective in order to create precise market segmentation both in market domains and technology areas:

#### 3.3.3.1 Vertical segmentation

The **vertical segmentation** offers goods and services to a specific industry, business, or a group of customers with similar needs. On the other hand, **horizontal segmentation** offers a broad range of goods and services to a wider group of customers with a wide range of needs.

On the **vertical axis** for this project there are 4 main markets targeted which correspond to the 4 project pilots, as it is essential to provide proven results that our solution can enhance different types of SMEs operating in a range of market sectors and offering diverse products and services, against threats and risks introduced by the recently adopted ICT advances:

- Smart-City.
- Internet of Things (IoT).
- e-Voting.
- Smart Grids.

##### 3.3.3.1.1 IoT

INTERNET OF THINGS - IoT. Image source: www.unsplash.com

Market size in 2022 : 561.04 USD Billion

Growth rate : 26.9%

Estimated number EU SMEs : 2 074 010

Estimated EU SMEs market share : 35% (64.83 USD Billion)

Type of SMEs : Consulting, System integrators, Application providers

*"Solutions aim to detect and prevent possible risks to structures and infrastructures by monitoring their operations and status in real time. These solutions are essential for ensuring that the assets' operations are maximally optimal, safe and cost competitive"*[4].

4 Grant Agreement-740787-SMESEC

The **Internet of Things (IoT) [32]**market size is expected to grow from **USD 170.57 Billion in 2017 to USD 561.04 Billion by 2022,** at a Compound Annual Growth Rate **(CAGR) of 26.9%.** Eurosmart on November 2016, in the report "Internet of trust, security and privacy in the connected world" estimates that about 10000 projects are ongoing on a global scale. All forecasters expect an exponential growth in the future years thanks to the potential value leveraging of the concept.

Bringing intelligence in existing and future infrastructures, in any activity field (watches, cars homes, plants …), the market players focused in past years on convenience features. Once the proof of concept and experiments clearly validated, time is now on reliability and one of the main challenge is security. Data is the "new gold" and all companies estimates that security and privacy issues are a fundamental basis for IoT development. From servers, networks to devices, the increasing number of entry points may compromise the full system if specifications, design and implementation are not fully secured. On our existing IT systems, the IoT introduces an added layer for sensing, sometimes also based on emerging technologies, specific low energy communication protocols that could considered as any doorway to attack the whole system. Any other layers (network, service, interface/application) can be reached from any unsafe device.

The market size is large enough to expect a subsequent role of SMEs in the Internet of Things revolution. Rethinking paradigms, creating value by bringing data intelligence tools, the SMEs are notably driving changes: Verizon in "State of the market: Internet of Things 2016"[33] estimated that in 2016, IoT startups will generate two or three times more funding than their consumer counterparts.

#### 3.3.3.1.2 Smart city

SMART CITY. Image source: www.unsplash.com

Market size in 2022 : 1.201 USD Billion

Growth rate : 23.1%

Estimated number od EU SMEs : 708 971

Estimated EU SMEs market share : 50% (285 USD Billion)

Type of SMEs : Start ups, Hardware manufacturers, Application developers

*"Provides the tools that activate citizen's creativity, imagination and communication, engages urban thinking and improves the relationship between citizens, the city municipality and city's public services. With their own communication devices (mobile phones) or via an application, citizens can post in real time issues and problems for something that happens in their city and inform their fellow citizens as well as the municipality for problems and incidents that occur every moment"*[5].

5 Grant Agreement-740787-SMESEC

The **Smart Cities Market (global) [34]** size is expected to grow from **USD 424.68 Billion in 2017 to USD 1,201.69 Billion by 2022**, at a **CAGR of 23.1%** during the forecast period.

Smart cities offer wide opportunities by concentrating urban services and fostering intelligence within networks. Urban applications of IoT technologies necessarily imply a broad range of areas (energy, building and infrastructures, mobility, governance, education, healthcare …) where interconnection of each network potentially unleash the data value potentials. In a 2016 report, "Cyber security, A necessary pillar of Smart Cities"[35], authors agree on the fact that the risk landscape is consequently the widest with security and privacy concerns led by insecure hardware, a larger attack surface, bandwidth consumption issues, application risks. Sensitive data and the network scope in smart cities implies high stakes in security to ensure confidentiality, integrity and availability as simple bugs may hinders huge impacts.

The smart city implementation involves a variety of stakeholders, combining institutional, physical, social and economic infrastructures. In that emerging market, SMEs intends to play a key role. In a May 2017 report named "Who will lead Smart Cities?" King&Wood Mallesons[36] depicted a pioneer role of SMEs bringing the key building blocks of smart cities on diverse areas. Even if they are not able to offer leadership in the field, small & medium sized companies will bring most of the main disruptive technologies and ideas with functional features based on concrete applications fields.

#### 3.3.3.1.3 Smartgrid

SMART GRID. Image source: www.unsplash.com

Market size in 2022 : 50.65 USD Billion

Growth rate : 19.4%

Estimated number EU SMEs : 14 739

Estimated EU SMEs market share : 46% (5.56 USD Billion)

Type of SMEs : Consulting, System integrators, Application providers

Similar fields : Water, Gas, Oil

*"Energy networks that can automatically monitor energy flows and adjust to changes in energy supply and demand accordingly. When coupled with smart metering systems, smart grids reach consumers and suppliers by providing information on real-time consumption".*

*"They can also help to better integrate renewable energy and also open up the possibility for consumers who produce their own energy to respond to prices and sell excess to the grid"[29].*

The **smart grid [30]** global market size is projected to grow from **USD 20.83 billion in 2017 to USD 50.65 billion by 2022**, at a Compound Annual Growth Rate (CAGR) of 19.4%.

European smart grid market revenue is expected to grow at a CAGR of 8.6% from 2015 to 2025 reaching almost 30Bn USD, Demand response will be the fastest growing segment within the European smart grid market with a 10-year growth rate of 17.6%., according to “Frost & Sullivan European Smart Grid Market Overview”.

This area offers wide potentials and fallouts to respond to sustainable development by ensuring field evolution, able to combine multi-sources of energy, inform alert and predict to properly adjust production to real-time consumption. Technically speaking, this implies to rethink the current networks, implementing sensors, smart counters, breakers, in production, distribution and in consumption / end users layers. This increase of potential vulnerable entry points raises security and privacy issues with unauthorized networks access, data spilling of private data, consumtion frauds or any malicious activities. The electricity network remains sensitive activities where security is crucial and especially in energy supply towards civil or militarian activities, health, water supply, food, communication. Any service breakdown may have high consequences on other dependant fields.

In the value chain, the sector is characterised with a high concentration of assets, capital that does not allow any SMEs actors as end users. But in this traditional sector, the need for change will opens new opportunities for small players and especially for SMEs in consulting, system integrators, application providers or any ICT solutions SMEs.

#### 3.3.3.1.4 E-Voting

E-VOTING. Image source: www.unsplash.com

Estimated number EU SMEs : around 34

Type of SMEs : Consulting, System integrators, Application providers

One of the most critical environments from the point of view of security is the electoral processes. To ensure privacy and integrity of the votes, electronic voting systems usually implement advanced cryptographic protocols at application level by implementing end-to-end encryption and verifiability of the election results, which detects if there have been any attacks. However, these measures do not prevent possible attacks[6].

[6] Grant Agreement-740787-SMESEC

As a niche market, there is no accurate and updated information about the market size. Based in Austria, E-Voting.CC provides a long list of key players. This is not an exhaustive list but the evoting activity seems to count about 50 companies[39]

In addition, with legal and political constraints, for a real development, the security aspects remain the first barrier. Trust and acceptance cannot be gathered without a strong guarantee in security, privacy and transparency in the voting process. The needed security level is such that the end to end security is a must to ensure reliability of voting activities. This implies security measures for data, system, transactions, VPN and associated networks.

#### 3.3.3.1.5 Other fields

To extend this vertical axis other areas can also be mentioned as part of the initial segmentation to keep them in the radar as emerging markets:

Also, apart from these four pilots, SMESEC will organize an **Open Call** in the final year of the project to invite more SMEs operating in diverse contexts and offering various kinds of services and products. This open call will allow SMESEC to collect additional evaluation results and make the necessary adjustments towards a robust and flexible security framework capable of supporting companies and organizations with limited budget. This first focus on pilots aims to start the SMESEC awareness, approaching market players with a vertical validated framework. That is a first step and the consortium will progressively extend to other fields. The following figure (Figure 8) gives the number of SMEs in Europe depending on their activity.

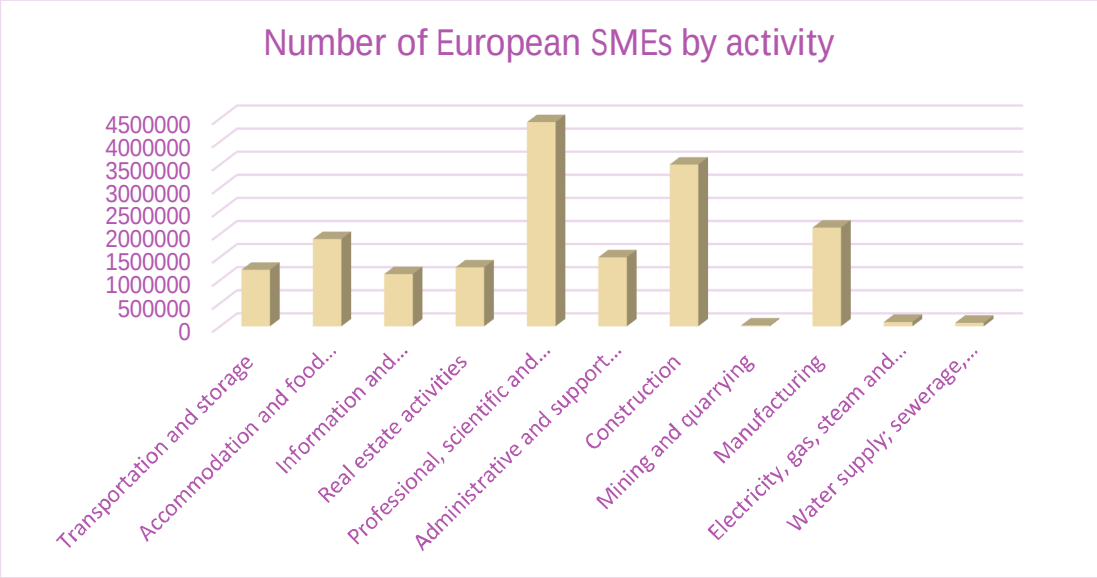


**Figure 8: SMEs landscape in Europe by activity – Source: Own creation/ Eurostats data**

This combined approach (vertical and horizontal) try to investigate the wider SMEs audience and also refers to the way the SMESEC identified solutions for market needs. This is confirmed by the latest Eurosmart report[42] on IoT security where some best practices are disseminated. Figure 9 shows the preconized action canvas.

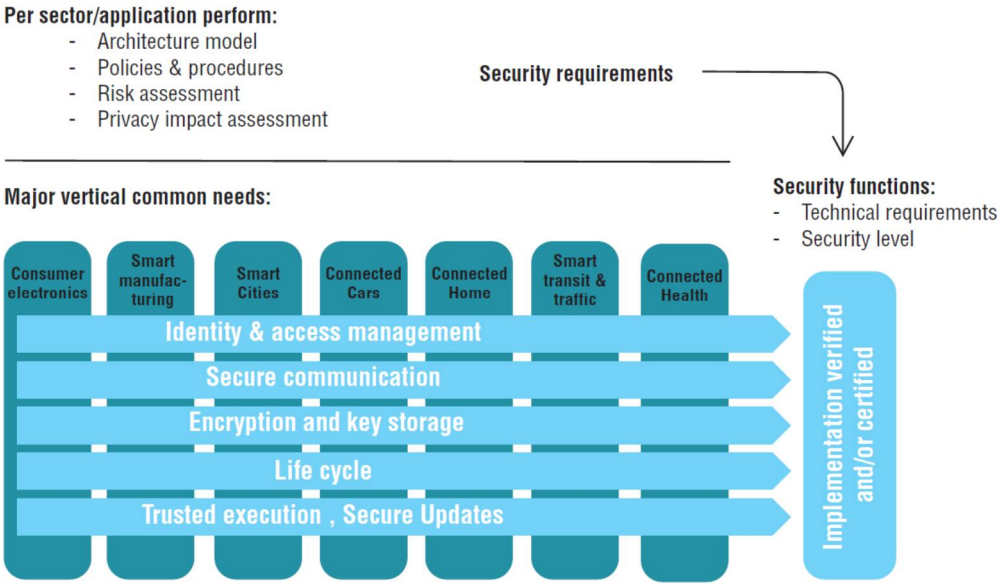


**Figure 9: Best practices approach for security development – Source Eurosmart report**

### 3.3.3.2 Horizontal segmentation

The **horizontal axis** will include all main security product areas SMESEC aims to provide a service as part of the project scope:

- User Entity Behaviour Analytics (UEBA).
- Cloud Access Security Brokers (CASB).
- Endpoint Detection and Response (EDR).
- Deception technology.
- Secure Web Gateway.
- Application security testing.
- Endpoint Protection Platform (EPP).
- Web application platform.
- Distributed DDoS.
- Intrusion detection and prevention systems.
- Security Information and Event Management (SIEM).
- Unified threat management.
- Governance risk management compliance.
- Other.

An extensive analysis on these traditional and emerging markets has been carried out in another project deliverable (D2.1 SME security characteristics description, security and market analysis). The following information will show the global market volume forecast for the next 3 years' period and the Compound Annual Growth Rate of each market segment:

- The **global user and entity behavior** analytics market is estimated to grow from USD 131.7 million in 2016 to USD 908.3 million by 2021, at a CAGR of 47.1% between 2016 and 2021 [16].
- The **global cloud access security brokers** market size to grow from USD 3.34 billion in 2015 to USD 7.51 billion by 2020, at a compound annual growth rate (CAGR) of 17.6% [17].

- The **endpoint detection and response** (EDR) market size is estimated to grow from USD 749.0 million in 2016 to USD 2,285.4 million by 2021, at an estimated Compound Annual Growth Rate (CAGR) of 25.0% [18].
- The **deception technology** market size is estimated to grow from USD 1.04 billion in 2016 to USD 2.09 billion by 2021, at an estimated Compound Annual Growth Rate (CAGR) of 15.1% [19].
- The **global SWG** market to grow from $2.20 billion in 2015 to $5.60 billion by 2020, at a Compound Annual Growth Rate (CAGR) of 20.5% during the forecast period [20].
- The **security testing** market is estimated to grow from USD 3.31 billion in 2016 to USD 7.61 billion by 2021, at a Compound Annual Growth Rate (CAGR) of 18.1% [21].
- The **Endpont Security** market is estimated to grow from USD 11.62 billion in 2015 to USD 17.38 billion by 2020, at an estimated Compound Annual Growth Rate (CAGR) of 8.4% from 2015 to 2020 [22].
- The **distributed denial of service** (DDoS) protection market size is estimated to grow from USD 824.4 million in 2016 to USD 2,162.9 million by 2021, at an estimated Compound Annual Growth Rate (CAGR) of 21.3% [23].
- The **global IDS/IPS security** market is estimated to be **$2.716 billion in 2014 and is expected to grow to $5.042 billion in 2019**. This represents an estimated Compound Annual Growth Rate (CAGR) of 13.2% from 2014 to 2019 [24].
- The **security information and event management** (SIEM) Market worth USD 4.54 billion by 2019 [25].
- The **global unified threat management** market is estimated to be $2584.6 million in 2014 and is expected to grow to $4445.7 million in 2019. This represents an estimated Compound Annual Growth Rate (CAGR) of 11.5% from 2014 to 2019 [26].
- The **eGRC** market size is expected to grow from USD 22.14 billion in 2017 to USD 43.87 billion by 2022, at a Compound Annual Growth Rate (CAGR) of 14.7% [27].
- The **identity & access management** market is estimated to grow from USD 8.09 billion in 2016 to USD 14.82 billion by 2021, at a CAGR of 12.9% between 2016 and 2021 [28].

Those areas are susceptible to be review and modified (add or remove) along the project's lifetime as the impact for targeted SME's can vary or even the results obtain could show there is not a viable transfer to market with a significant economic impact.

## 3.4 Stakeholders analysis

One of the standard analysis to be carried out in a market analysis is the stakeholder analysis. The key activities to perform on this subject include:

- Start identifying who they are.
- Get a deeper understanding of the different identified stakeholders and start mapping and understanding their positioning around SMESEC project. This could include but is not limited to evaluating their degrees of influence, degree of importance, and their points of interest and prioritizing them.

To strengthen the analysis, it would be beneficial to directly interact with stakeholders and to revaluate the analysis and potentially consider a more mature Stakeholder Model.

At this initial stage the SMESEC project has identified three main stakeholders' groups:

- **Active stakeholders**, who take part in the SMESEC environment (they are either a part of the 'consumption' of SMESEC services or providing SMESEC services (development, maintenance, consultancy, etc.).
- **Enabling stakeholders**, who add or provide to the expansion and use of SMESEC framework (who would be a part of dissemination of this technology –media- or policy, subsidy, or regulations makers that would promote or recommend consumers and providers into using this technology -Public Institutions-.
- **Internal stakeholders**, involved in the development and establishment of SMESEC (consortium partners).

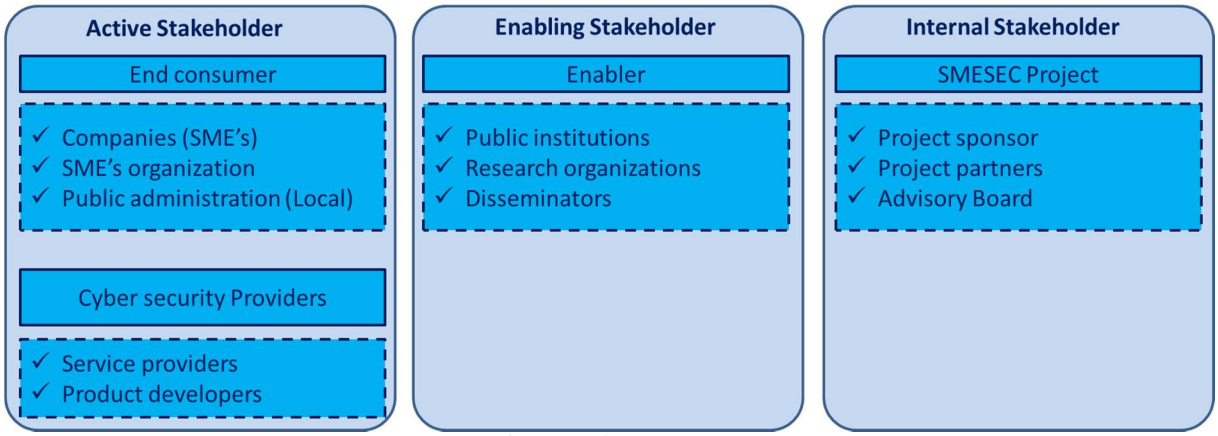


**Figure 10: Identification of SMESEC stakeholders[31]**

Of course, there are many ways to distribute the different types and categories of stakeholders, as illustrated in the Figure 10, however, at this initial stage of the project this seems like the first analysis of what the potential stakeholders could be.

The methodology proposed for this stakeholder mapping is based on the Mendelow's matrix[38], where the initial approach for the four quadrants considered (as per in the basic diagram below, Figure 11) includes:

In **Monitor Quadrant**, these stakeholders are expected to need minimum effort and are easily influenced due to their lack of power and interest. They are sometimes also called the 'Crowd', which are more considered to be 'potential' than actual stakeholders. (**service providers, product developers,** etc.)

For the **Keep Satisfied Quadrant**, these stakeholders are considered the context setters and need to be informed. They are people who have high power, but maybe little interest. With their high-power attribute, if their interest can be piqued it could lead to an influence of the overall future context. (**public institutions, research organizations, etc.)**

For the **Keep Informed Quadrant**, these stakeholders are considered the subjects. They have Low Power, but High Interest. If their

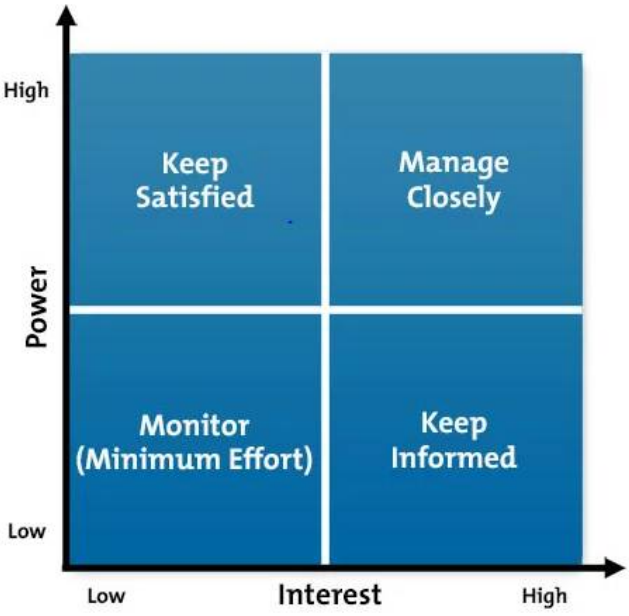


**Figure 11: Mendelow's stakeholder matrix**

Interest is used as a catalyst to motivate them to increase their 'power', they could move to the Players Category and become a key part of the Stakeholders. (**SME's, Local administrations, etc.)**

In the **Manage Closely Quadrant**, these stakeholders are expected to be the players. They have both high interest, power, and are our most valuable asset. They should obtain the greatest effort to maintain their satisfaction. (**Project sponsor, SME's organizations [37], etc.)**

This initial approach will be reviewed during the project lifetime to keep this influence matrix updated in order to help the consortium to redirect effort on one or several influence groups.

# 4 Project dissemination

## 4.1 Dissemination strategy

### 4.1.1 Approach

The dissemination activities will be developed under the work package 6 and especially the task T6.2 that firstly aims at designing and launching a coherent and organised project dissemination plan. It coordinates the network of contacts of each entity to reach end-user communities (including SMEs), the public sector, and the wider public. It also launches and carries out the project dissemination activities with valuable end-user contacts and groups of interest.

The dissemination plan has been developed based on the SMESEC project proposal and market analysis and by consulting the SMESEC partners. Each partner has contributed with suggestions for channels that should be used and can be served by the SMESEC consortium. In the SMESEC project, each partner will have an active role and contribute in dissemination activities. FHNW will coordinate all partners contributions, ensuring the relay of these actions on project channels in web pages, social networks, etc. and organizing the effective implementation and update of the dissemination plan. EGM will enable and review the results that are being achieved.

The section here describes the project dissemination plan, the overall strategy as depicted in Figure 12, the channels used for dissemination, the dissemination kits and artefacts, and the dissemination process and monitoring for Year 1. The remaining years will be described in the deliverables D6.2 at M12 and D6.2 at M24.

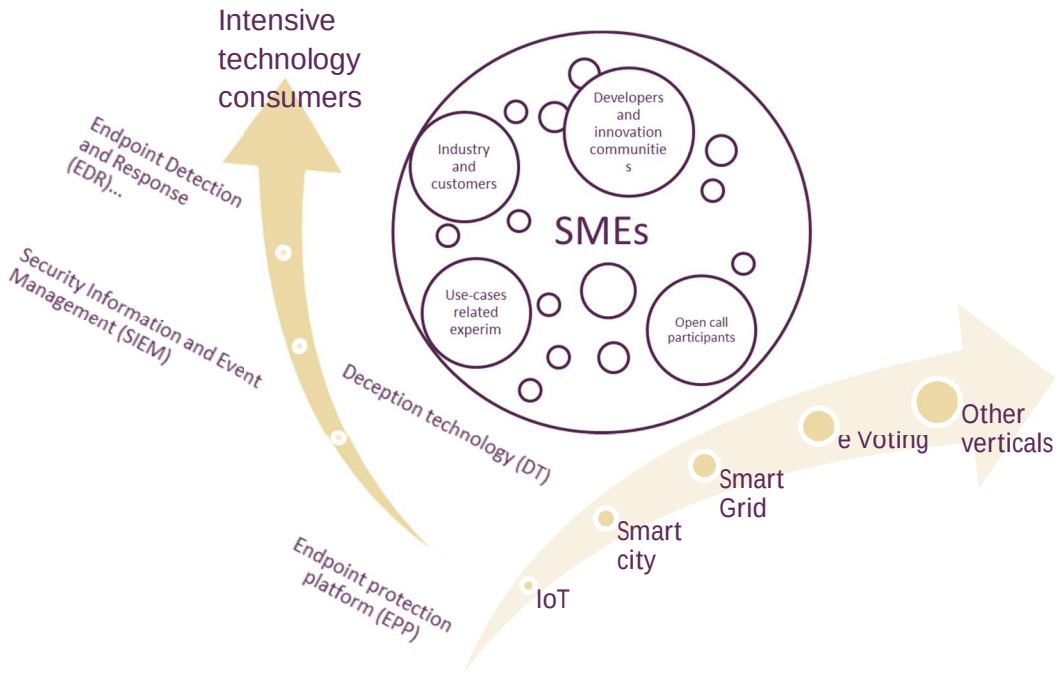


**Figure 12: Overview of SMESEC dissemination approach**

#### 4.1.1.1 Objectives

The dissemination plan will serve as a support activity for all the work performed during the SMESEC project, complying with specific expected impacts as shown in Figure 13. From a short-term view, it firstly intends to ensure a proper communication of all project outcomes and generates project awareness and attractiveness towards future users, SMEs, etc. From a mid-term view, these actions will support standardisation and exploitation activities and trigger the adoption and implementation of SMESEC security framework while ensuring the wider project audience.


**Figure 13: Overview of SMESEC dissemination objectives**

Chronologically speaking, the dissemination plan will address the following objectives:

- Promote project visibility and awareness:
  - Establish the needed communication tools for the consortium partners.
  - Broadcast key messages in targeted communities.
  - Collect market feedback, create and expand the network of contacts.
- Disseminate the project results:
  - Prepare the needed basis for exploitation and standardisation.
  - Release the first SMESEC results and progress.
  - Promote the open call process and sustain adoption of SMESEC framework by SMEs.
- Implement the project outcomes:
  - Engage SME end-user communities in the SMESEC project results.
  - Extend project scope enhancing adoption of other fields.

### 4.1.2 Dissemination phasing

Figure 14 gives an overview of the dissemination plan and how it is aligned with the SMESEC project plan.

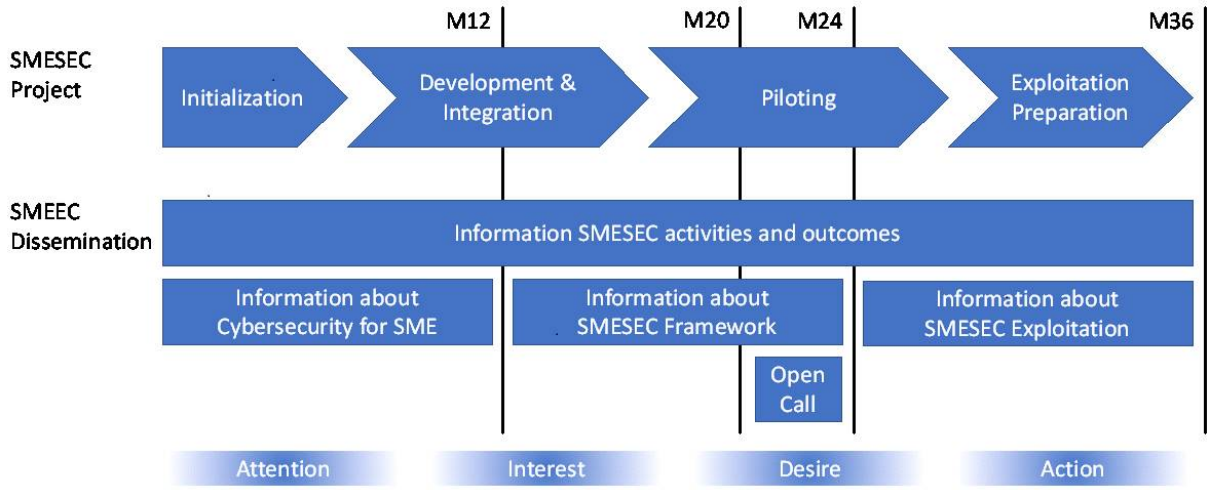


**Figure 14: Dissemination plan**

Table 3 describes the dissemination plan that is aligned with the SMESEC project plan. The plan consists of a series of phases that lead to the recruitment of open call participants and SMESEC framework users upon the initiation of exploitation. For each phase, the table shows the matching dissemination objectives and the measurements utilised to judge the success of the dissemination.

| Dissemination phase | Disseminated SMESEC results | Dissemination objectives | Success measurements |
|---|---|---|---|
| M01-M36: Information | In this phase SMESEC offers expertise. | Inform industry, academia, citizens, and politics about SMESEC activities and outcomes. | Awareness of SMESEC project by external stakeholders. |
| M06-M12: Attention | | The audience is aware of cybersecurity for SME, including the problems and solutions. | Awareness of SMESEC topic by product-oriented roles in SMEs of different levels of maturity. |
| M12-M24: Interest | In this phase, SMESEC offers results that can be explored and tested. | The audience wants to learn about the SMESEC framework. | Audience's size is large enough for Open Call (M20) and SMESEC framework adoption (M24). |
| M24-M34: Desire | | The audience wants to join workshops and try the SMESEC framework and | Enough registrations for Open Call (M24) and 100 SMEs adopt the SMESEC framework |

| Dissemination phase | Disseminated SMESEC results | Dissemination objectives | Success measurements |
|---|---|---|---|
| | | experience its impact. | (M34). |
| M30-M36: Action | In this phase, SMESEC exploitation is being initiated. | The audience wants to use the exploitable results of the SMESEC framework and sustain the use. | All Open Call Members (M30) and 100 SMEs are active users of the SMESEC framework (M36). |

**Table 3: Dissemination plan**

Both, the open call participants and SMESEC users will be recruited by following the AIDA approach: Generating attention on cybersecurity for SMEs, interest in the SMESEC framework, the desire to try the framework, and encouraging the actions of registering as a user and sustaining the framework use.

SMESEC dissemination prepares dissemination kits and artefacts for digital channels and three levels of involvement in events and exhibitions.

- High involvement: presence with a booth
- Medium involvement: presentation, talk or workshop participation at the event
- Light: participation and distribution of flyers

### 4.1.3 Targets

#### 4.1.3.1 Overall approach

The dissemination performed by the SMESEC project is primarily intended to support the validation and exploitation of the SMESEC framework according to the SMESEC business model. For dissemination, a particularly important validation activity will be the open call. Figure 15 gives an overview of the SMESEC business model.

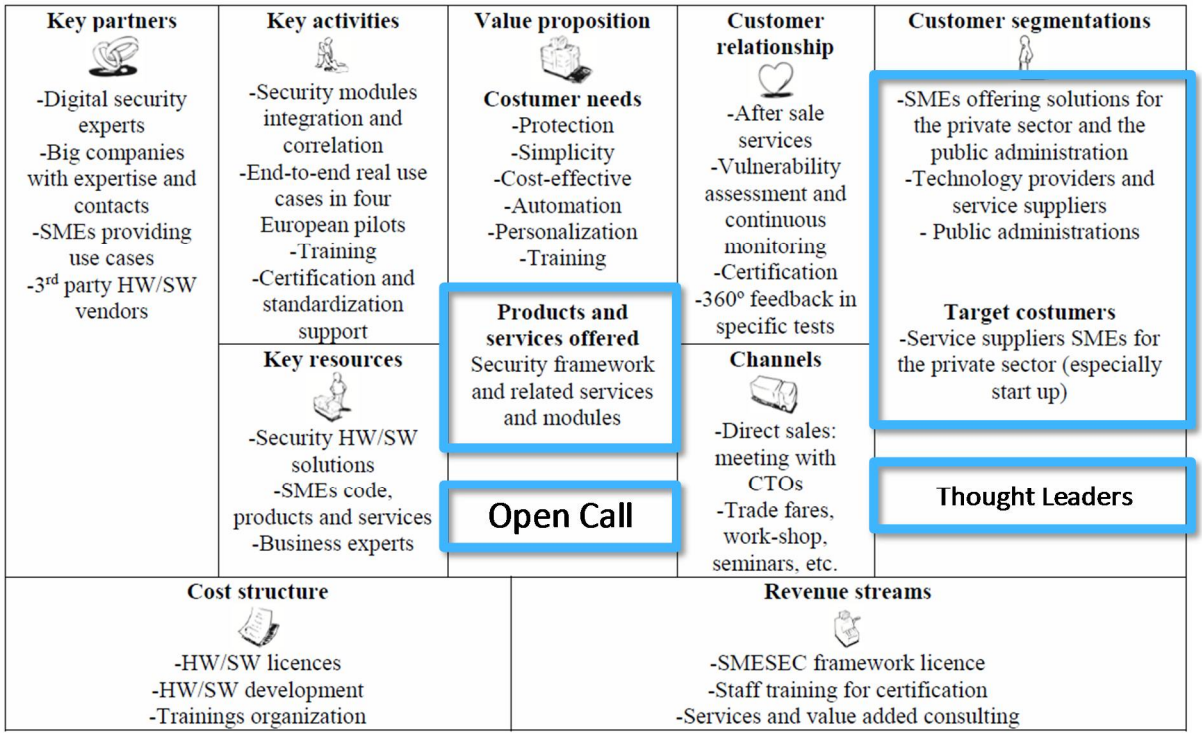


**Figure 15: SMESEC business model (thick blue frames: priorities for dissemination).**

Table 4 shows the target audiences that the SMESEC dissemination is trying to reach. The target audiences will be addressed with refined messages based on the market and stakeholder segmentation described earlier in this document. The focus of SMESEC dissemination is small and medium-sized enterprises. That target is prioritised over the other target.

| Target | Dimension | Segments | Information needs | Desired outcomes |
|---|---|---|---|---|
| SME | Size | Small | Goal-Oriented Approach for Hardening a Digital Offering | Use and endorse SMESEC Framework |
| | | Medium-sized | Goal-Oriented Approach for Cybersecurity in Organization | |
| | Maturity | Start-up | Top-10 Hardening of a Digital Offering | |
| | | Established | Sustaining Cybersecurity for the whole Digital Portfolio | |
| | Domain | IoT | IoT-Specific Chapters | |

| Target | Dimension | Segments | Information needs | Desired outcomes |
|---|---|---|---|---|
| | | 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 innovations | Papers and citations |
| | | Technology | Technology-oriented communities | |
| | | Engineering | Security engineering for SMEs | |
| Policy | Region | EU | Policy recommendations | Encourage SMESEC-enabled cybersecurity practice. |
| | | Switzerland | | |
| | | Israel | | |
| R&I | Region | EU | Recommendations for economic development | Offer calls allowing SMESEC to mature and grow. |
| | | Switzerland | | |
| | | Israel | | |
| Individuals | Specialization | Opinion Leaders | Business-enablement with SMESEC. | Disseminate information about SMESEC Framework |
| | | Employees | SME protection and safety with SMESEC. | Use and endorse SMESEC Framework |
| | | Public | Trust in protected SMEs. | Positive attitude towards SMESEC |
| Standardi-zation | Body | ETSI | | Use SMESEC Results in Standards |
| | | IETF | | |

**Table 4: Dissemination target groups**

#### 4.1.3.2 SMEs segmentation

SMESEC, as a security-related project, addresses a wide range of potential domains of SMEs. On the exploitation side, SMEs are the key target groups for SMESEC technology adoption, on the market or in open call processes. Each dissemination activity will be tailored to the specific group according to the specific message to be conveyed. In the following, we describe the segmentation of addressed SMEs based on their main field of activity and value chain positioning.


**Figure 16: The SMESEC use cases ranked by market potential size**

The vertical uses cases of SMESEC are a way to validate the SMESEC framework based on industry-specific requirements. They are also a lever that will serve dissemination purposes. The consortium will firstly focus on the main use cases' areas of IoT and Smart City, creating links with key market players in these booming fields. Through open calls, SMESEC will progressively extend the project scope by including other sectors such as environment, water, retail, agriculture, automotive, healthcare, and tourism.

The SMESEC partners worked on a general system architecture that describes the value chain positioning of the SMESEC use cases. This value chain allows fine tuning the segmentation. The figure below shows the main components in the data chain where SMESEC brings assets and progress to ensure secure device, secure communication, secure cloud.

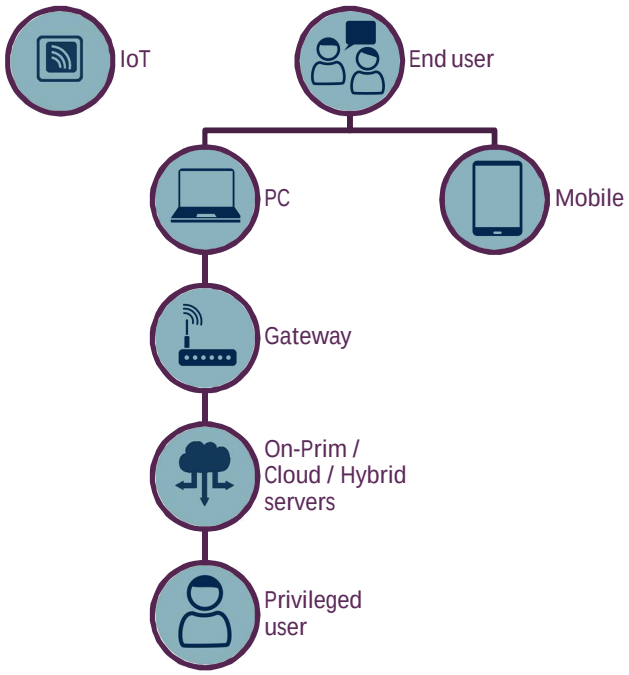


**Figure 17: SMESEC use cases, overall system architecture**

The architecture covers multiple system layers, including sensing, network, middleware, and application layers. Figure 17 shows this architecture. The Internet of Things use case offers the longest chain in this architecture. It allowed us to identify the following target groups:

- Device manufacturers.
- End-Users and customers.
- System integrator.
- Consultants.
- Applications developers.
- Cloud service providers.
- Manufacturer of testing equipment.
- Security certification agencies.

SMEs offering products and services will be targeted with tailored messages corresponding to layer-specific needs.

#### 4.1.3.3 SMEs, Experimenters, end users target groups

The SMESEC framework will foster a cyber-secure ecosystem towards existing SMEs solutions considering both technology providers and developers as mapped in Figure 18. The dissemination strategy will focus primarily on the developer community and SMEs. The partners already established contact with the above target groups within the project consortium. Participation in events and demonstration activities will extend this basis to build a wider audience and support SMESEC exploitation with links to the market players.

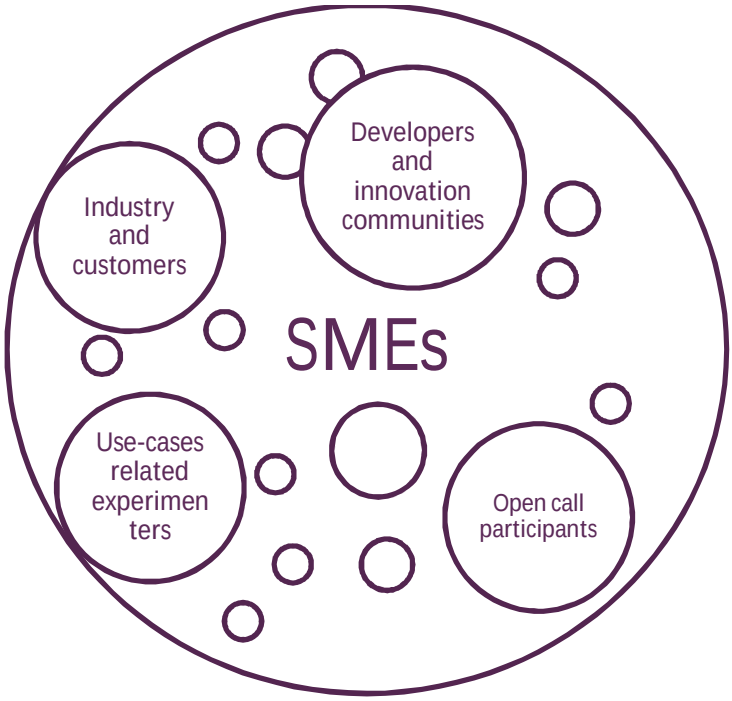


**Figure 18: SMESEC experimenters target groups**

##### 4.1.3.3.1 Industry and customers

The SMESEC dissemination will focus on the benefits to be gained by the industries that become active agents for testing and developing the SMESEC solutions. Industry partners will be activated by establishing contacts with industry associations, business support organizations, promotion organisations, and industrial organisations specific to European regions.

##### 4.1.3.3.2 Developers and innovation communities

Dissemination will also target independent developers and entrepreneurs to show the flexibility of the solutions developed by SMESEC and stimulate the creation of new, innovative and secure applications. The activities for this target group will be based on the organisation of and participation in events such as innovation fairs, technology road-shows, and hackathons. Furthermore, engagement of this group will be sought through participation in conferences and workshops within the security and ICT sector.

#### 4.1.3.4 Other target stakeholders

In a wider view, we identified key and other target groups that are not necessarily future users of SMESEC solutions but offer perspectives for disseminating results and obtaining access to markets and SMEs networks the SMESEC partners are not active in at this moment. This approach will give a larger audience and bring additional relevancy to SMESEC communication.

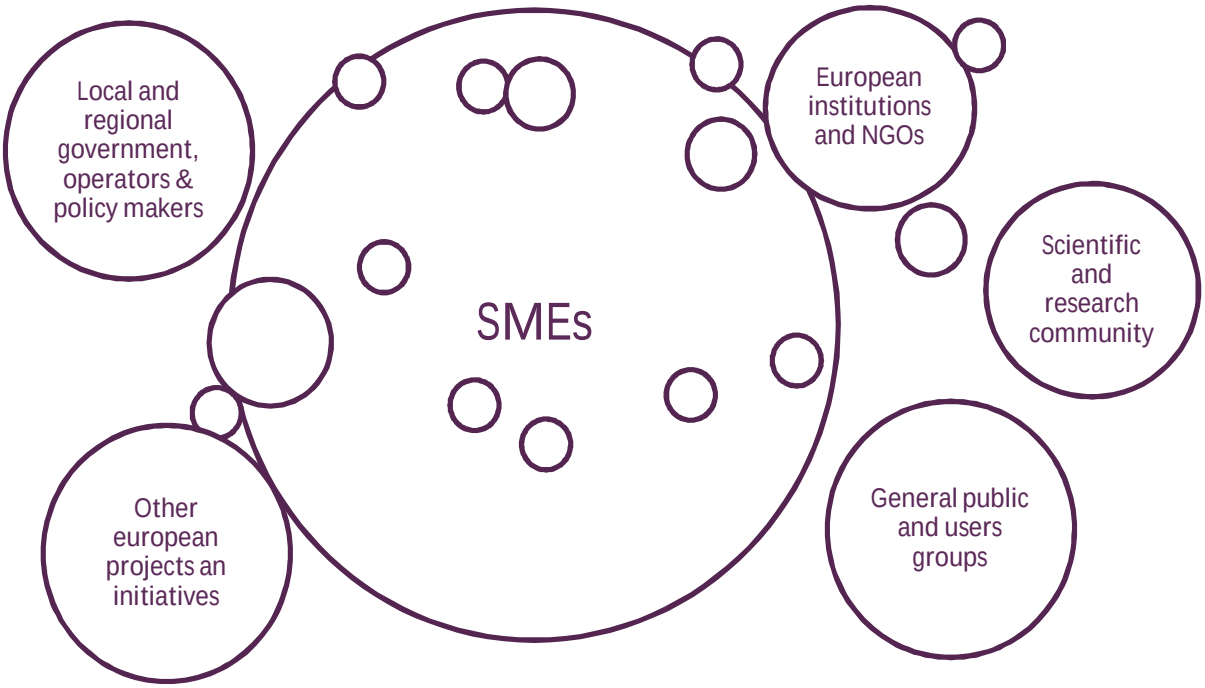


**Figure 19: SMESEC stakeholders target groups**

##### 4.1.3.4.1 Local and regional government, operators & policy makers

Dissemination will focus on developing contacts with officials and policymakers that play a key role in security and SMEs asset management policy and decision-making at various levels. Dissemination will here be done through direct personal contact, newsletters, and participation in related events. Relevant stakeholders in this target group include city councils, public and private partnerships for a coordinated contingency plan, authorities and companies that provide control services, and regional development agencies or their equivalent.

##### 4.1.3.4.2 Scientific and research community

Dissemination to this group will focus on disseminating the innovation on technological and business aspects. Dissemination will here be done through European and international conferences and workshops, scientific newsletters, magazines, and website articles. Links and synergies with other regions and regional actors will also be sought.

##### 4.1.3.4.3 European institutions and NGOs

Dissemination to this group will focus on European institutions, non-governmental organizations (NGOs) and on other European regional bodies that are either involved in the SME business or

provide relevant services. The approach for identifying representative bodies is to look for those that overlap with the issues for each participating region, thus multiplying their efforts and impact.

#### 4.1.3.4.4 General public and user groups

Dissemination activities will target general public and users groups. The general public includes citizens, commuters, and tourists. The user groups include communities active in environmental policies, citizens safety organisations, and special interest groups such as the European Cities and Regions Networking. SMESEC will raise awareness about cybersecurity threats and encourage the targets to investigate and try the SMESEC framework. The dissemination activities will focus on how the SMESEC outputs can support the reliability, security, sustainability and efficiency of SMEs business management locally and how this could positively impact the quality of life for European citizens. In this respect, the dissemination material will be provided on specific media outlets, such as news, magazine articles and web portals, and via planned dissemination events.

#### 4.1.3.4.5 Other European projects and initiatives

The transfer of knowledge and experience within the European projects in overlapping fields is a primary requirement of the SMESEC dissemination activities. This transfer enhances the unity of the European research taskforce and increases the innovation impact of SMESEC. Dissemination will be performed through the participation of the SMESEC partners in other projects regarding cybersecurity.

### 4.1.4 Dissemination Messages

The dissemination will be implemented with a series of contents or stories that are kept consistent across channels. They include:

- Cybersecurity problems for SMEs.
- SMESEC framework vision.
- Interviews with stakeholders.
- Demonstration of SMESEC use by use cases.
- SMESEC releases.
- SMESEC Open Call.
- SMESEC success stories.

The dissemination messages are based on WP2, WP3, WP4, and WP5 results and evolve as the project progresses. Table 5: Dissemination message shows the message to be communicated by SMESEC dissemination.

| **Theme** | **Messages** | |
|---|---|---|
| Importance of cybersecurity for SMEs | 60% of SMEs experienced a cybersecurity breach or attack in 2016.<br>68% of SMEs have no systematic approach to ensuring cybersecurity.<br>40% of SMEs would struggle to recover from data loss, 20% would not be able to. | |
| Threats of importance for SMEs | DoS and DDoS<br>Vulnerable Software<br>Broken Authentication<br>Misconfigurations<br>Injection | Cross-Site Scripting<br>Sensitive Data Exposure<br>Garbage Data<br>Malicious Insiders |

| Theme | Messages |
|---|---|
| Goals of Cybersecurity for SMEs | Cybersecurity must…<br>…be based on up-to-date facts and events<br>…be available to any employee<br>…work even in a busy, hectic, and diverse environment |
| SMESEC Framework | Training and Awareness Offering<br>Definition and Recommender Tools<br>Discovery and Resolution Tools<br>Protection and Response Tools<br>Lessons from Framework Testing and Validation |
| SMESEC Methodology | Framework Tested on Real-World SMEs in…<br>…IoT<br>…Smart City<br>…Smart Grid<br>…e-Voting<br>…Digital Start-ups |
| Advantages of SMESEC | Get cybersecurity right even when doing it yourself<br>Build cybersecurity with just little investment<br>Work without complicated formal policy and procedures |

**Table 5: Dissemination message**

Figure 20 and Figure 21 illustrate the elements of the storytelling approach to the cybersecurity problem of SMEs. A specialised designer will create the visualisation. The presentation of the stories will be kept consistent with the SMESEC project branding.


**Figure 20: SMESEC Story-telling board on cybersecurity stakes for SMEs**

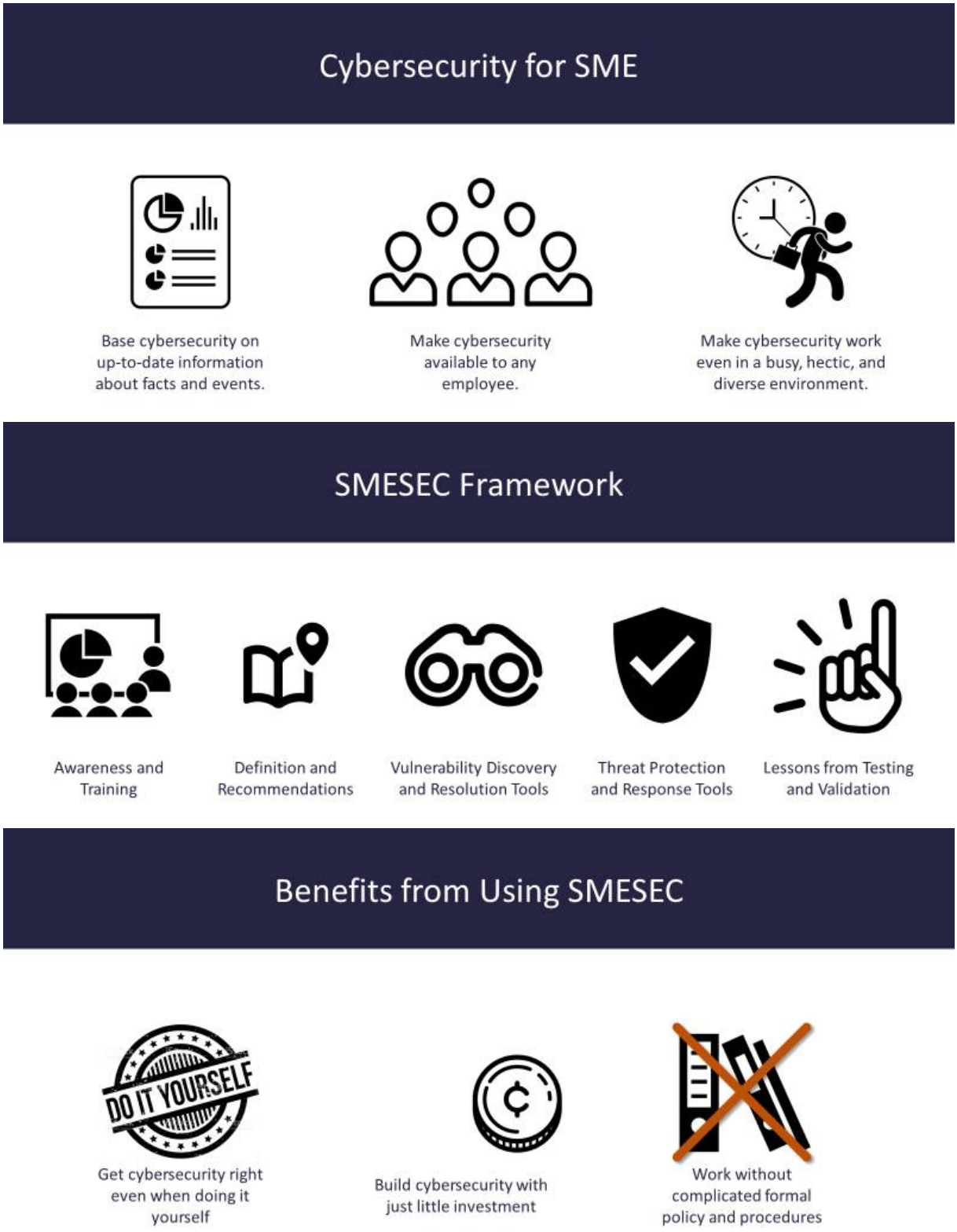


**Figure 21: Story-telling board on SMESEC presentation and benefits**

The core values being pursued with the design are: trust in SMESEC, respect of the expertise of the SMESEC consortium, and simplicity of the SMESEC framework. A professional designer is packaging these values in the visual design used to communicate the SMESEC message to the target audience.

## 4.2 Dissemination kits and artefacts

### 4.2.1 Project branding

#### 4.2.1.1 Project logo

To set the project visual identity, a dedicated logo was designed to sum up the SMESEC features. The acronym typology and police colours game foster the direct understanding of the project scope with its two key ideas “SME” AND “SEC”, contraction of security (Figure 22).


**Figure 22: SMESEC logo**

The illustration helps to understand the project with a padlock that is associated with security concept. The logo further contains graphs or building profiles depending on the point of views. These two elements refer to smart cities or IoT use cases.

#### 4.2.1.2 Visual identity

The project logo codes are transcribed in the project template with a set of colours that will be used in the deliverables with a dedicated template and communication materials as presented in Figure 23. The resulting consistency aims to foster the project awareness, giving a standardised visual presentation for all project deliverables and outcomes presentations.


**Figure 23: SMESEC Color palette**

Figure 24 illustrates the project branding approach.


**Figure 24: SMESEC project branding.**

### 4.2.2 Public website

SMESEC offers a webpage for information about the SMESEC project and dissemination of results. It will contain all information about the series of contents that are used to disseminate during the project lifetime. The webpage can be reached on www.smesec.eu.

Figure 25 shows the current SMESEC webpage. The webpage provides general information about the SMESEC project with the static content Home, About, Consortium, Funding, and Legal Notes and the dynamic information News, Events, Publications, and Deliverables. To enhance community building and strengthen project emulation, the website offers a set of pointers with Contact, Links to Social Medias and Subscription. The website's security is hardened with the SMESEC approach, thus offers dependability to its users and an additional use case to the consortium.


**Figure 25: SMESEC webpage**

The webpage is undergoing revision to follow the story-telling approach shown in Figure 20 and Figure 21. It will be enriched in the coming months with continuous news and events update, use cases presentation based upon the validated project graphical branding. The following enhancements will be offered with interactive features on the homepage:

- What are the cyber threats to SMEs? Icons are being selected to reflect the intuition of the SME end users. Hovering over the icons and texts will expand a definition of the threats. A click will lead to blog entries by the respective cybersecurity experts. The result aims at educating the SME and building trust in the SMESEC expertise.
- Cybersecurity for SME: Adapt messages to photos with SME representatives stating the cybersecurity issues. A click on the photo will lead to blog entries featuring the full interview with the SME representative.
- SMESEC Framework: Evolve according to the definition of the SMESEC framework, which will be delivered by WP3. A click on a tool will lead to a product sheet (minimum) or an experience report (maximum).
- The Voice of SMEs: The short statements will be refined with interviews of the concerned people. The statements will be linked to blog entries featuring the interviews and, if applicable, use case videos.

Specific developments will be set to deliver a membership space within 2019 offering newsletter subscription, member section with SMESEC framework access for open call selected SMEs.

### 4.2.3 Promotional materials

To support the dissemination of project outcomes, the consortium defined a set of promotional materials for communication towards the target groups.

The Figure 26 and the Table 6: Dissemination Material gives an overview of the material types that SMESEC is preparing to support partners over time in dissemination activities. The material is intended to be produced by professional designers, and a budget is being reserved for its production. The first preliminary set will be updated in early 2019 to ensure the effectiveness of communication activities, tuning the dissemination messages depending on experience feedbacks from SMESEC partners in trade fairs, conferences, workshops or any event or exchange with the relevant communities.

| Material | Number | Purpose | Timing |
|---|---|---|---|
| Website | 1 | Information about SMESEC and access to SMESEC framework in member section | Website: Q3 2017<br>Member section: Q3 2108 |
| Press Kit | 3 | Material for public press to write about SMESEC | Update after each milestone |
| Infographic | 2 | Use on webpage, flyers, and roll-up | Q1 2018<br>Q1 2019 |
| Flyer | 1 | Material for events | Q1 2018 |
| Roll-Up | 2 | Material for events | Q1 2018<br>Q1 2019 |
| Booth | 1 | Material for events | Q1 2018 |
| Video | 5 | 1 project vision and 4 use case videos demonstrating use and benefit of SMESEC | Q1 2018 |
| Webinars | 2 | Material used for explaining use and benefits of SMESEC Framework | 2018/2019 |
| Tutorials | 2 | Material used for explaining use and benefits of SMESEC Framework | 2018/2019 |

**Table 6: Dissemination Material**

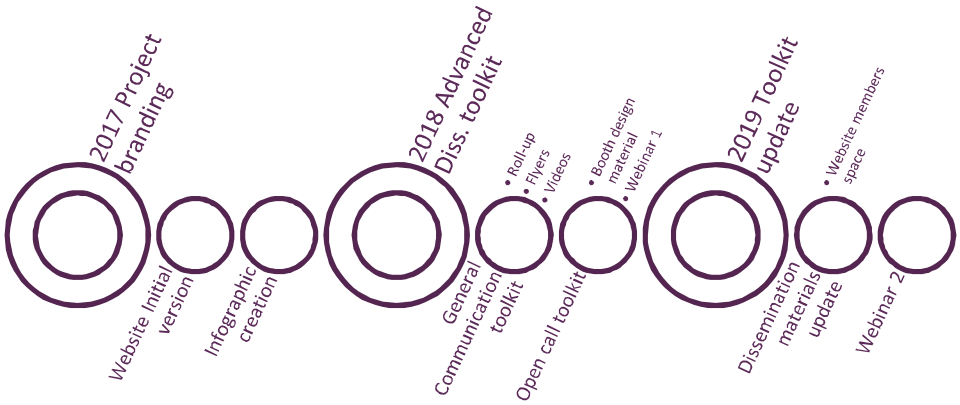


**Figure 26: Phasing of the project dissemination toolkit**

### 4.2.4 Social networks

Along the project, the consortium will disseminate within social networks, creating, managing and animating communities on Twitter, Facebook and LinkedIn. Table 7 gives an overview of the social channels served by SMESEC.

| Type | Indicators Objective |
|---|---|
| Twitter | https://twitter.com/SMESEC_EU |
| Facebook | https://www.facebook.com/smesec.eu/ |
| LinkedIn | https://www.linkedin.com/groups/13532696 |

**Table 7: SMESEC social channels**

These channels, presented in Figure 27, will serve as relays for website posts (e.g. news, events announcement, etc.) and be managed by each partner, publishing insights on the topics addressed by SMESEC and especially in Cybersecurity, IoT, Smart city, Smart grid, eVoting, and digital Startup, bringing interactions by reacting, exchanging during conferences and external events.

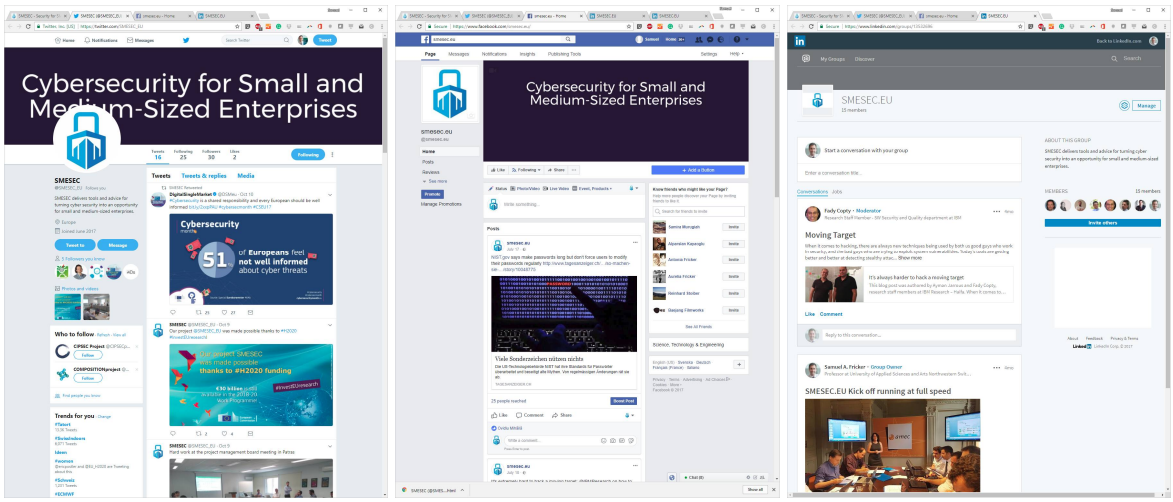


**Figure 27: Snapshots of the SMESEC presence on social channels**

## 4.3 Dissemination channels

The dissemination plan is based on dissemination channels. The dissemination will be designed as a blend of activities from one or more channels used to reach the respective target groups. The dissemination is responsible for communication of the project results towards stakeholders, potential customers, interested communities and other relevant audiences that, in one way or another, might participate in the adoption of the project results.

This section gives an overview of dissemination channels intended to be used by SMESEC, including academic, industrial, policy, EU Research and Innovation, and citizen-oriented channels.

### 4.3.1 Industrial Channels

#### 4.3.1.1 SMESEC activities and events

##### 4.3.1.1.1 General publications

SMESEC will publish press releases and articles in specialised trade newspapers & magazines. It will provide news and newsletters, including a periodic awareness newsletter that will be sent to interested parties.

#### 4.3.1.2 SMESEC Partners' Channels

The consortium will also use social media for the dissemination of information and leverage the existing channels of SMESEC partners. Table 8 gives an overview of the channels that SMESEC partners are serving.

| Type | URL | Partner |
|---|---|---|
| Twitter | https://twitter.com/Scytl_SA | SCYTL |
| | https://twitter.com/Worldsensing | WOS |
| | https://twitter.com/IBMResearch | IBM |
| Magazine | ATOS Spain Corporate Magazine | ATOS |
| Blog, newsletter | https://securityintelligence.com/ | IBM |
| | http://ascent.atos.net/ | ATOS |
| | WOS newsletter and new at the company website | WOS |
| Other | ATOS internal scientific community | ATOS |
| | WOS internal engineering community | WOS |

**Table 8: SMESEC partners' channels**

##### 4.3.1.2.1 Workshops and training sessions

SMESEC will organise focused workshops and training events and invite the European and international communities to discuss issues of interest for the project.

During the project, two workshops will be organised by the academic partner FORTH. These workshops will be performed in conjunction with major conferences in the field, to give further visibility to the SMESEC activities. Since academic partners in SMESEC are both involved in the TPC and Organization Committees of flagship conferences in the field, SMESEC can easily organise such workshops.

To produce an immediate market impact, the SMESEC partners EGM and UoP will also organise two training courses for the SME technicians and staff. With these events, SMESEC will provide valuable information to the technical persons that in the coming future will have the responsibility to apply the security methodologies offered by SMESEC.

#### 4.3.1.3 External events

SMESEC will participate in major industrial and trade events to give presentations and distribute project dissemination material. Specifically, events with a large potentially interested audience will be targeted. This presence will be associated with project networking with security-related organisations, offering potential access to SMEs networks. Both presentations and provision of leaflets constitute main vehicles for dissemination and exploitation.

Table 9 gives an overview of industrial events that are intended to be served with SMESEC results. Each year, SMESEC intends to be present at three big events. In total, partners will attend or participate in 50 events, workshops, seminars, conferences where partners will create opportunities to offer project presentations and results dissemination.

| Discipline | Event | Attendees | URL | Place |
|---|---|---|---|---|
| Cybersecurity | European Information Security Summing (TEISS) | 450 | https://biztechevents.co.uk/teiss/ | London |
| | CyberCentral Summit | 900 | https://cybercentral.eu/ | Prague |
| | Security of Things World | - | http://securityofthingsworld.com/en/ | Berlin |
| | Cybersecurity Europe | - | http://www.cybersecurity-europe.com/ | London |
| Technology | Mobile World Congress | 108’000 | https://www.mobileworldcongress.com/ | Barcelona |
| | IoT Solutions World Congress | 13’000 | http://www.iotsworldcongress.com/ | Barcelona |

| Discipline | Event | Attendees | URL | Place |
|---|---|---|---|---|
| | IoT Week – Global IoT Summit | - | http://iot-week.eu/ | Bilbao |
| | Internet of Things World UE | 13'000 | https://tmt.knect365.com/iot-world-europe/ | London |
| | SIDO | 7'500 | http://www.sido-event.com/ | Lyon |
| | Industry of Things World | 1'000 | http://industryofthingsworld.com/en/ | Berlin |
| | Digital Festival | - | http://digitalfestival.ch/ | Zurich |
| Startup | Web Summit | 60'000 | https://websummit.com/ | Lisbon |
| | Seedstars Summit | - | https://www.seedstarsworld.com/summit/ | Lausanne |
| | Unconvention | | | Brussels |
| | Lift Conference | 4'000 | http://liftconference.com/ | - |
| Innovation | Patras Innovation Quest (Patras IQ) | | http://www.patrasiq.gr/ | Patras |

**Table 9: Conferences and Forums**

Table 10 gives an overview of networks, associations, and promotional organisations that are intended to be served with SMESEC results.

| Discipline | Network, Association, Organization | URL | Partner |
|---|---|---|---|
| Smart Cities | EIP Smart Cities | https://eu-smartcities.eu/ | EGM |
| | EU SmartCities Cluster | https://www.smartcitiescluster.eu | EGM |
| Startup | Startup Europe | http://startupeuropeclub.eu/ | FHNW |
| | Orange Grove Patras | http://orangegrovepatras.biz/ | CITRIX |

**Table 10: Networks, Associations, Promotional Organizations**

The SMESEC consortium has a strong dedication to the promotion of open source software. This commitment is driven by the belief that open source software contributes to the development and goals

of European society as a whole. Specifically, it benefits students in their quest for learning, young entrepreneurs in their business plans, SMEs and large industry in cutting costs, and therefore European citizens and the member states in general. Parts of the developed products will be released as open source using the appropriate licenses. Care will be taken so that the selected licenses will not prevent commercialization of new products and services that use our open source software. All relevant details are included in the Consortium Agreement. Table 11 gives an overview of open source networks and communities that are intended to be served with SMESEC results.

| Discipline | Network, Community | URL | Partner |
|---|---|---|---|
| Cybersecurity | Open Software Security Community (OWASP), including local chapters | https://www.owasp.org/index.php/Switzerland | FHNW |
| | swissICT Information Security Society Switzerland (ISSS) | https://www.isss.ch/home/ | FHNW |
| | Security Interest Group Switzerland | https://www.sig-switzerland.ch/de/ | FHNW |
| | Beer on Tuesday, Swiss Hacker Meetups | https://www.beerontuesday.ch/ | FHNW |

**Table 11: Open source networks and communities**

### 4.3.2 Academic Channels

Scientific publications in leading journals and presenting the project's outcome in conferences and workshops either as keynotes or regular presentations will be considered as an important way to disseminate and exploit the results generated in SMESEC. Following the innovation management plan, quality management plan and data management plan, SMESEC results and deliverables will be published. Due to the importance of the topic, a high number of technical publications can be expected, boosting the visibility of the consortium. Potential publication venues include well-reputed journals and international conferences. Furthermore, the consortium aims to publish individual white papers, and to contribute in ongoing white papers by different research forums in the digital security domain (Such as 5G-PPP white paper on Cyber-security, etc.).

Table 12 gives an overview of the conferences that are intended to be served with SMESEC research.

| Type | URL | Partner |
|---|---|---|
| Cybersecurity | ACM Transactions on Privacy and Security (formerly: ACM Transactions on Information and Systems Security) | UU |
| | International Journal of Information Security | UU |
| | Information and Computer Security | UU |
| | IEEE Transactions on Dependable and Secure Computing | UOP |

| Type | URL | Partner |
|---|---|---|
| | Elsevier Journal of Information Security and Applications | UOP |
| Computing | IEEE Transactions on Service Computing | ATOS |
| | IEEE/ACM Transactions on Networking | ATOS |
| | Springer Service Oriented Computing and Applications Journal | ATOS |
| | Advances in Internet of Things | ATOS |
| Software Engineering | ACM Transactions on Software Engineering and Methodology | ATOS |
| | IEEE Transactions on Software Engineering | ATOS |
| | Information and Software Technology | FHNW |
| | Empirical Software Engineering | FHNW |
| | Requirements Engineering | FHNW |

**Table 12: Journals**

Table 13 gives an overview of the important conferences that are intended to be served with SMESEC research.

| Discipline | Conference | Partner |
|---|---|---|
| Cybersecurity | International Conference on Security and Cryptography (SECRYPT) | SCYTL |
| | Nordic Conference on Secure IT Systems (NORDSEC) | SCYTL |
| | IEEE European Symposium on Security and Privacy | UOP |
| | IEEE International Symposium on Hardware-Oriented Security and Trust (HOST) | UOP |
| | Cyber-Tech Israel | IBM |
| Computing | The International Conference for Electronic Voting (E-Vote-ID) | SCYTL |
| | Euromicro Conference on Digital System Design | UOP |
| Software engineering | IEEE/ACM International Conference on Software Engineering (ICSE) | ATOS |
| | International Conference on Information Systems (ICIS) | UU |
| | European Conference on Information Systems (ECIS) | UU |
| | IEEE International Requirements Engineering Conference (RE) | FHNW |
| | Product-Focused Software Process Improvement (PROFES) | FHNW |
| | Empirical Software Engineering and Measurement (ESEM) | FHNW |

**Table 13: Conferences**

Table 14 gives an overview of the important working conferences and workshops that are intended to be served with SMESEC research.

| Discipline | Conference | Partner |
|---|---|---|
| Cybersecurity | International Conference on Information Security Theory and Practice (WISTP) | FORTH |
| | International Symposium on Research in Attacks, Intrusions, and Defenses (RAID) | FORTH, UOP |
| | International Workshop on Security and Trust Management (STM) | SCYTL |
| | Workshop on Evolving Security and Privacy Requirements Engineering (ESPRE) | IBM |
| | Haifa Security and Privacy Research Seminar | IBM |
| | Swiss Cyberstorm | FHNW, SCYTL |
| | B-Sides Zurich | FHNW |
| | Black Alps | FHNW |
| | Area41 Security Conference | FHNW |
| | Requirements Engineering: Foundation for Software Quality (REFSQ) | FHNW |

**Table 14: Working conferences and workshops**

### 4.3.3 Other Stakeholders Channels

#### 4.3.3.1 Policy and standardisation related channels

Table 15 shows a list of dissemination events that are intended to be served with SMESEC results and recommendations.

| Discipline | Conference, Forum | Partner |
|---|---|---|
| Cybersecurity | European Organization of Security (EOS) | ATOS |
| | International Cyber Security Protection Alliance (SCPA) | ATOS |
| | International Workshop on Trustworthy Embedded Devices (TrustED) | ATOS |
| | International Conference on Trust, Privacy and Security in Digital Business (TrustBus) | ATOS |
| | International Conference on Digital Society (IDCS) | ATOS |

| Discipline | Conference, Forum | Partner |
|---|---|---|
| Research | European Researchers' Night (NIGHT) | FORTH |

**Table 15: Conferences and forums**

Further is planned to investigate European and national institutions, regional bodies, and NGOs. Examples are councils, public-private partnerships, authorities, and development agencies.

Table 16 gives an overview of the newsletters that are intended to be served with SMESEC results and recommendations.

| Discipline | Newsletter | URL | Partner |
|---|---|---|---|
| Cybersecurity | Cybersecurity and privacy digital newsletter managed by EC | https://ec.europa.eu/digital-single-market/en/newsletters | FHNW |

**Table 16: Newsletters**

Table 17 gives an overview of other channels that are intended to be served with SMESEC results and recommendations.

| Discipline | Channel | Partner |
|---|---|---|
| Cybersecurity | European Cyber Security Organization (ECSO) | ATOS<br>EGM |
| | Open Software Security Community (OWASP) | FHNW |

**Table 17: Other channels**

An overview of the standardisation bodies, SMESEC is intending to collaborate with is developed in the chapter Target standards developing organizations (SDOs). A full list of available standardization bodies in the field of information and cybersecurity is provided in section 5.3

#### 4.3.3.2 EU Research and Innovation related channels

Table 18 gives an overview of European projects that are intended to be served with SMESEC results. Projects like CIPSEC may organise workshops where SMESEC presence is possible.

| Discipline | Project | Partner |
|---|---|---|
| Cybersecurity | ARMOUR | ATOS |
| | Unicorn | FORTH |
| | CIPSEC | UoP |
| | EUNITY | FORTH |
| | CERTCOOP | FORTH |

| Discipline | Project | Partner |
|---|---|---|
| | SHARCS | FORTH |
| | 5GINFIRE | UOP |
| | FASTPRK2 | WOS |
| | mF2C | FORTH |
| | NECOMA | FORTH |
| | SYSSEC | ATOS |

**Table 18: Projects**

Table 19 gives an overview of the COST actions that are intended to be served with SMESEC results.

| Discipline | COST Action ID | Action name | Partner |
|---|---|---|---|
| Cybersecurity | IC1403 | CRYPTACUS | UOP |
| | IC1306 | CryptoAction | UOP |

**Table 19: COST actions**

Table 20 gives an overview of the support actions that are intended to be served with SMESEC results.

| Type | Support action | URL | Partner |
|---|---|---|---|
| Cybersecurity | Cyberwatching | https://www.cyberwatching.eu/ | ATOS |
| Digital Single Market | CloudWatchHub | http://www.cloudwatchhub.eu/smes | ATOS |

**Table 20: Support actions**

## 4.4 Roadmap

Table 21 describes the detailed dissemination plan for the first year. The plan aims to support the dissemination phases Information and Attention with the help of presences in conferences, the SMESEC blog and the SMESEC social channels. Starting from M12, the dissemination actions will encourage registration on the webpage to support framework validation and later framework use.

| Target | Activity | Event / Channel | Date | Success measurement |
|---|---|---|---|---|
| Any | Website | www.smesec.eu | Jul 2017 | - |
| Any | Twitter, Facebook, LinkedIn | smesec.eu | Jul 2017 | - |
| SME | Talk | Cyberstorm | Oct 2017 | Blog and social channel followers |

| Target | Activity | Event / Channel | Date | Success measurement |
|---|---|---|---|---|
| SME | | TEISS | Feb 2018 | Blog and social channel followers |
| SME | Light participation | Mobile World Congress | Feb 2018 | Blog and social channel followers |
| Policy | Newsletter | Single-Market Newsletter | Feb 2018 | Blog and social channel followers |
| SME/ Startup | | Start Summit 2018 | Mar 2018 | Blog and social channel followers |
| SME/IoT | Booth | SIDO | Apr 2018 | Blog and social channel followers |
| SME/ Startup | | Seedstars Summit | Apr 2018 | Blog and social channel followers |
| SME | Light participation | CyberCentral Summit | May 2018 | Blog and social channel followers |
| SME/IoT | Medium | IoT Week | Jun 2018 | Blog and social channel followers |
| SME/IoT | Light participation | Internet of Things World EU | Jun 2018 | Blog and social channel followers |
| SME | Medium | Security of Things World | Jul 2018 | User registrations |
| SME | Medium | Patras IQ | Aug 2018 | User registrations |
| SME | Light participation | Industry of Things World | Sep 2018 | User registrations |
| SME/IoT | Booth | IoT Solutions World Congress | Oct 2018 | User registrations |
| SME | Light participation | Cybersecurity Europe | Oct 2018 | User registrations |
| SME/ Startup | | Lift Conference | Nov 2018 | User registrations |
| SME/ Startup | Website | Web Summit | Nov 2018 | User registrations |

**Table 21: Achievements 2018 and detailed dissemination plan for the year 2018.**

## 4.5 Dissemination processes

To guarantee continuous collective awareness of project goals and progress, the SMESEC partners implemented a set of measures to facilitate internal communication, partners' synchronisation and impact tracking. In addition to the meetings and teleconferences, a dedicated "ownCloud", shared online repository and a methodology has been defined for all dissemination activities to guarantee the knowledge sharing and generate synergies.

### 4.5.1 Dissemination Activities toward SMEs

The dissemination activities toward SMEs include presentations at conferences, press releases, non-scientific publications such as popular magazines and trade journals, flyers, blog posts, and trade fair booths. We here provide a summary of the relevant provisions of the Consortium Agreement, a tool to submit an activity, as well as an overview of the activities of the Consortium.

**Approval of Dissemination Activities**

Consortium members shall seek prior approval of the release by the Consortium before the dissemination of results:

- Prior notice of any planned activity shall be given to the other Parties at least 45 days before the dissemination.

- Any objection to the planned activity shall be made in writing to the Coordinator and the Party or Parties proposing the dissemination within 30 calendar days after receipt of the notice.

- If no objection is made within 30 days from the date of notification, the activity is permitted.

A form, named "Dissemination monitoring – Events and Papers", to notify the consortium of any publication is provided in the SMESEC OwnCloud repository in the dedicated work package folder.

### 4.5.2 Scientific Publications

These activities include regular or invited journal articles, proceedings of conferences, book chapters, and theses. We here provide a summary of the relevant provisions of the Consortium Agreement, a tool to submit a manuscript for a scientific publication, as well as an overview of the scientific publications within the Consortium.

Scientific publications are a common element of H2020 projects. Below you will find

- a summary of the relevant provisions of the Consortium Agreement;
- a tool to notify the Consortium about publications;
- an overview of all publication activities.

Scientific publications will be reported continuously to the EC.

These activities include regular or invited journal articles, proceedings of conferences, book chapters, thesis, etc.

**Approval of Scientific Publications**

Consortium members shall seek prior approval of the release by the Consortium before the dissemination of results:

- Prior notice of any planned activity shall be given to the other Parties at least 45 days before the dissemination.

- Any objection to the planned activity shall be made in writing to the Coordinator and the Party or Parties proposing the dissemination within 30 calendar days after receipt of the notice.

- If no objection is made within 30 days from the date of notification, the activity is permitted.

A form to notify the consortium of your publication is provided in the SMESEC ownCloud repository.

### 4.5.3 Dissemination Support

The dissemination support helps partners in the dissemination activities with logos, illustrations, and templates. This support material is available for download from the SMESEC ownCloud repository.

Each recorded dissemination activity will be advertised on the SMESEC homepage and the social media channels of SMESEC. Selected results will be made available in newsletters and press releases.

### 4.5.4 Acknowledgment of Funding

The following states the rules for the acknowledgement of funding for publications, presentations, press releases, patents, etc.

**Funding Body Acknowledgment**

Any dissemination or communication activity (in any form, including electronic) must (unless the funding bodies request or agree otherwise or unless it is impossible):

- display the EU emblem,

- display the SERI logo, and

- include the acknowledgement text.

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.

### 4.5.5 Dissemination monitoring

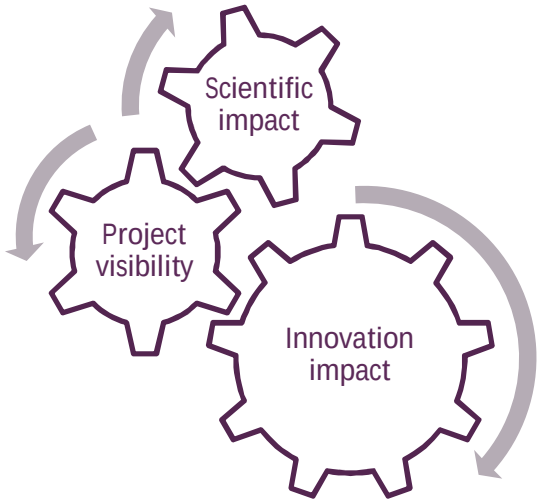


**Figure 28: SMESEC Dissemination impacts monitoring**

The dissemination activity (shown in Figure 28) will be continuously monitored with identified key indicators. With these quantitative results, in the light of qualitative feedbacks from partners, the consortium will yearly readjust the dissemination strategy to adapt it to markets and stakeholders needs. Three KPIs categories are set in the project to rationally assess the project visibility (awareness creation & support), innovation impact (results adoption & exploitation) and scientific impact (results dissemination). A set of new indicators is added (in grey colour in the following tables) to monitor the project attractiveness and especially on the website traffic and in social networks. No quantified objectives are defined for these items as they cannot be estimated at this stage, trends in time series will be analysed to confirm the dissemination orientation. All KPIs will be tracked and reported each month. General meetings are planned during the project aiming at presenting project progress each 6 months (at most) to specific targets, gather feedback, and provide insight to implement the successive iteration of project development, tests, and assessments.

| Channel | Indicators | Objectives |
|---|---|---|
| Website | Downloads per year | 1000 |
| | Unique visitors per month | 1000 |
| | Visits per month | 4000 |
| | Website news per month | 1 |
| Social networks | Social networks posts per month | 20 |
| | Twitter followers | 500 |
| | Facebook followers | 500 |
| | Linkedin group members | 500 |
| Publications / Communication materials / Contributions | Press releases | 4 |
| | Newsletters per quarter | 1 |
| Events | Attended exhibitions | 25 |

| Channel | Indicators | Objectives |
|---|---|---|
| | Webinars | 3 |
| | Tutorials | 3 |

Table 22: Visibility monitoring and related objectives

| Channel | Indicators | Objective |
|---|---|---|
| Publications / Communication materials / Contributions | Contributions to roadmaps | 2 |
| | Contributions to standards | 2 |
| | Contributions to policy | 2 |
| Events | Number of workshops | 2 |
| Website | Open call registrations | 20 |
| | Registered members (SMESEC framework users) | 100 |

Table 23: Scientific impact monitoring and related objectives

| Channel | Indicators | Objective |
|---|---|---|
| Publications / Communication materials / Contributions | Journal publications | 8 |
| Events | Conference talks | 20 |
| | Attended events | 50 |

Table 24: Innovation impact monitoring and related objectives

# 5 Evolving standardization

## 5.1 General approach

This chapter outlines the SMESEC standardization strategy, coordinated by Utrecht University (UU). This standardization strategy builds upon the existing UU maturity models for information security and cybersecurity, and is structured according to the standard system development lifecycle (SDLC). The corner stone of the SMESEC standardization strategy is the SMESEC maturity model for personalized advice and subsequent incremental process improvement within SMEs throughout Europe. The model is accompanied by a reference implementation – i.e. assessment engine – to help improve its sustainability and relevance well beyond the SMESEC project timespan as depicted in Figure 29.

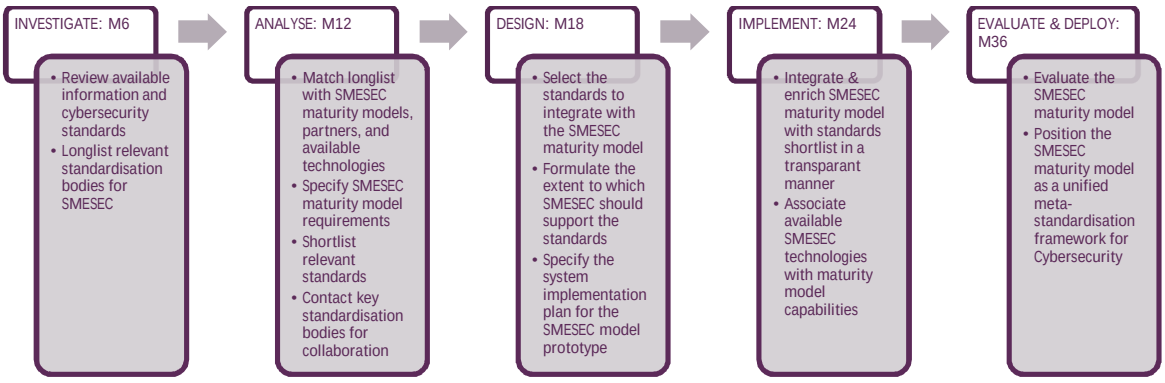


**Figure 29: Overview of the SMESEC Standardization plan with five main phases, each consisting of several steps.**

First, in the INVESTIGATE phase during M1-M6 we have explored the abundance of available standardization bodies related to information and cybersecurity. This resulted in a longlist of standards which are elaborated upon below in section5.4.1.2.

Second, in the ANALYSE phase from M7-M12 we match the longlist of available standards with the SMESEC maturity models, partners, and available technologies. In parallel, we engineer the requirements for the envisioned SMESEC maturity model, including transparent standards lineage, implementation technology guidelines per capability, and maturity model maintainability-by-design, among others. These two steps result in a shortlist of security standards most relevant for SMESEC. We will contact these key standardization bodies to discuss collaboration opportunities.

Third, in the overlapping DESIGN phase from M10-M18 we select the standards to integrate with the SMESEC maturity model, and formulate the extent to which SMESEC should support the standards. At the same time, we develop a technical specification for the IT implementation plan to more efficiently and effectively prototype the model adhering to the specified requirements.

Fourth, in the overlapping IMPLEMENT phase from M13-M24 we implement the technical specification to more efficiently and effectively prototype the model iterations while adhering to the specified requirements. The resulting prototype integrates and enriches the original UU/SMESEC maturity models with the standards shortlist in a transparent and sustainable manner, while associating

the available SMESEC technologies from all SMESEC partners with the appropriate maturity model capabilities. Note that piloting the model will already be possible at this stage using a paper-based version. However, a flexible and maintainable analytic system implementation of the encompassing SMESEC maturity model is considered crucial for a long-lasting SMESEC impact.

Fifth, in the EVALUATE & DEPLOY phase in M25-36 we evaluate the final SMESEC maturity model in our four case studies and possibly other environments to fine-tune its many aspects as appropriate. After a satisfactory evaluation, we will start positioning the SMESEC maturity model as a unified meta-standardization framework for cybersecurity in especially SMEs, that we expect to be received well by all stakeholders, thanks to its transparent meta-standards design, associated toolkit to help implement the personalized security advices, and the support of the standardization collaborators which we already contacted in phase 2.

## 5.2 Objectives

The standardization plan outlined above operationalizes the SMESEC T6.3 Standardization activities. The main goals of this plan are: **First,** to disseminate the SMESEC solution and promote the adoption of existing or emerging standards and cyber-security models specially defined for SMEs, ensuring our development will be consistent with the standards, and within the community making our outcomes available. **Second**, to provide feedback to the standardization bodies to help them to improve their standards and interoperability. Provide tools and methods to evaluate implementation (conformity, etc.). **Third**, to create links with active standardization bodies and participate in evolving standards, pushing the SMESEC results.

## 5.3 Target standards developing organizations (SDOs)

The SMESEC project implies a wide range of areas where the standardization activities aim to contribute in. From the project features, with a similar approach as done in dissemination, a list of main players has been created to identify targets among International organization for Standardisation, ETSI, OneM2M and European Commission Directives and regulation.

This first work, developed in the next sections (Investigation phase) enables us to build an overall landscape for SMESEC standardisation plan. The Figure 30 below shows the standardisation scope and target SDOs, involved in cybersecurity or more specifically involved in verticals contributions for IoT, Smart cities and Smart grids fields.


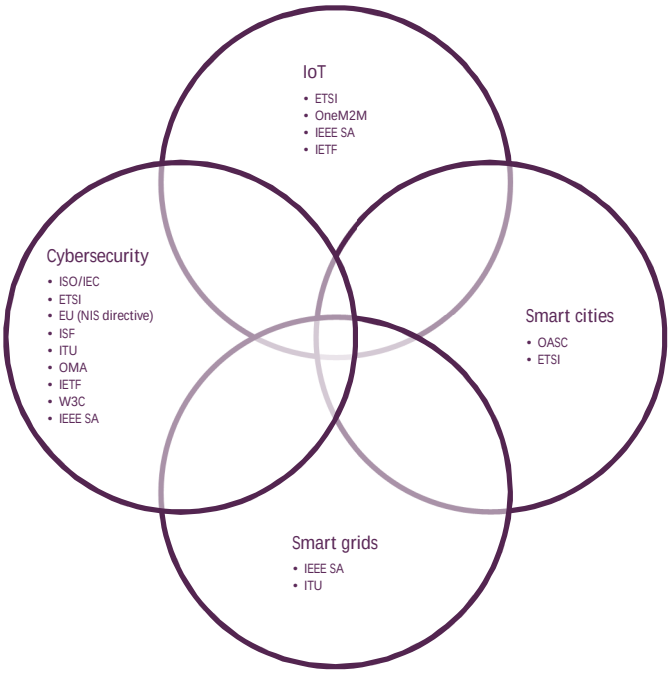


**Figure 30: SMESEC related SDOs landscape**

## 5.4 Standardization phases

In the sections below we describe in more detail the realization of the Evolving Standardization plan.

### 5.4.1 INVESTIGATE phase: M1-M6

The Information Security Focus Area Maturity (ISFAM) model by Spruit & Roeling (2014) is one of the core components of the envisioned SMESEC model. It effectively showcases the type of activities that need to be performed to realize the envisioned SMESEC model, as shown in Table 25. Therefore, as a first step in SMESEC we expand and update our exploration of potentially relevant security-related standards and best practices.

The ISFAM model has already been satisfactorily evaluated in Telecom, Logistics, Finance, and Healthcare. Similarly, the Cyber Security Focus Area Maturity (CYSFAM) model by Spruit & Lingen [40] integrates various cybersecurity standards, and it has been proven to be valuable in Finance.

The modelling approach for these models has been developed at Utrecht University over the past decade as Focus Area Maturity models, which can be interpreted as improved Capability Maturity Model Integrated (CMMI) models (e.g. [41]). A FAM model is more flexible, more granular, and incorporates interdependencies between focus areas, all of which are crucial to the SMESEC framework goals. This architecture allows for personalized advices through quick scans, in combination with the Characterizing Organizations' Information Security for SMEs (CHOISS) model by Mijnhardt, Baars, & Spruit (2016). Perhaps even more importantly, it provides a proven artefact architecture that can satisfy all SMESEC requirements.

| *IS focus area* | *CISSP* | *ISO 27K* | *ISO-light* | *ISF* | *IBM* | *ISFAM* |
|---|---|---|---|---|---|---|
| Risk management | X | X | X | X | | *Area 1* |
| Policy, laws & standards | X | X | X | X | | *Area 2* |
| Organization | X | X | X | X | | *Area 3* |
| HR security | | X | X | X | X | *Area 4* |
| Compliance | X | X | X | X | | *Area 5* |
| Identity/access management | X | X | X | X | X | *Area 6* |
| Software development | X | X | X | X | X | *Area 7* |
| Incident management | X (Disaster Rec.) | X | X | X | X | *Area 8* |
| Business continuity | X | X | X | X | | *Area 9* |
| Change management | X | Comm./Oper. Mgt | X | X | | *Area 10* |
| Physical/environmental | X | X | X | X | X | *Area 11* |
| Asset management | | X | X | X | | *Area 12* |
| Architecture | X (plus Design) | | | X | | *Area 13* |
| Malicious attacks (prevent) | | Partly | | X | | *Part of other areas* |
| Cryptography | X | Tool | | X | | *Part of malicious attacks* |
| Telecom./network security | X | X | X | X | | *Part of architecture* |
| Governance | X | Organization | Organization | X | X | *Part of organization* |
| Privacy | | | | X | X | |
| Transaction/data integrity | | | | X | X | *Part of other areas* |

**Table 25: Comparative analysis of information security areas in existing models with respect to the 13 ISFAM focus areas, from (Spruit & Roeling, 2014).**

#### 5.4.1.1 Findings: Review

Below we list our findings of the review of available information and cybersecurity standards and best practices, resulting in the longlist as presented in the next section.

Regarding ICT and Cyber Security Standardization Efforts in Europe, there are three European Standards Organizations (ESOs): CEN, CENELEC, and ETSI. The mission of the European Committee for Standardization (CEN) is to foster the European economy in global trading, the welfare of European citizens, and the environment. Through its services, it provides a platform for the development of European Standards and other technical specifications.

The European Standardization Organizations (CEN, CENELEC and ETSI), created in 2011, the Cybersecurity Coordination group to provide strategic advice on standardization in the field of IT security, Network and Information Security (NIS) and Cyber Security (CS). The Group was converted into CEN-CENELEC Focus Group on Cybersecurity in 2016.

Standardization activities in SMESEC will focus on the following areas related to four pilot SMEs: Cyber Security, IoT, Smart Grids, Smart Cities, and E-voting. Interestingly, these areas are also included in the EC Rolling Plan for ICT Standardization 2017, prepared by The European Multi Stakeholder Platform (MSP) on ICT.

Benefits of our SMESEC framework standardization activities include reduced qualification and certification costs (and thus reduced time-to-market for SMEs), improved security, improved interoperability for developing new products, and removal of system integration barriers.

Requirements, on the other hand, regarding our SMESEC framework include adherence to the existing relevant standards in order to become a reference platform for SMEs' cyber security. Therefore, the SMESEC partners will wherever possible:

- **Use standards and recognized open-source tools** in the development of the tools, the infrastructure of the proposed platform, user interfaces, APIs and data formats.
- **Contribute to standards and open-source tools**, with the insights and the outputs resulting from the implementation of the SMESEC framework.
- Give some focus on growing importance of **standards for open platforms** which are main driver for innovation by SMEs. So, they are promoted by EU also worldwide such as on EU PPP Flagship project FIWARE where +1000 SMEs are working with and IoT/oneM2M standardized platforms which will attract thousands of SMEs.

Both are necessary not only to maximize the impact of the SMESEC project but also to increase its marketability, in a domain where interoperability is a key selling point. Standardization is therefore an important objective of the project and the partners of SMESEC are highly engaged in standardization processes.

#### 5.4.1.2 Findings: Longlist

A preliminary list of the relevant standards bodies, and the standards most appropriate for the SMESEC contributions, is given below in Table 26 with a sample of potential SMESEC collaborators in the rightmost column.

| Committee Acronym | Committee name | Description | Collaboration with SMESEC partner(s) |
|---|---|---|---|
| ISO/IEC | International Organization for Standardization / International Electrotechnical Commission | The International Organization for Standardization is an international standard-setting body composed of representatives from various national standards organizations.<br>The International Electrotechnical Commission (IEC) is the world's leading organization that prepares and publishes International Standards for all electrical, electronic and related technologies. | UU |
| ETSI | The European Telecommunications Standards Institute | ETSI, the European Telecommunications Standards Institute, produces globally-applicable standards for Information and Communications Technologies (ICT), including fixed, mobile, radio, broadcast and Internet technologies. | UU, EGM, UOP |
| oneM2M | Standards for M2M and the Internet of Things | The purpose and goal of oneM2M is to develop technical specifications which address the need for a common M2M Service Layer that can be readily embedded within various hardware and software, and relied upon to connect the myriad of devices in the field with M2M application servers worldwide. | |
| NIS | Network and Information Security Directive | The NIS Directive is the first piece of EU-wide legislation on cybersecurity. It provides legal measures to boost the overall level of cybersecurity in the EU. | |
| ISF | Standard of Good Practice of the Information Security Forum | The Standard of Good Practice for Information Security 2016 (the Standard) provides comprehensive controls and guidance on current and emerging information security topics enabling organisations to respond to the rapid pace at which threats, technology and risks evolve. | UU |
| ITU | International Telecommunication | ITU is the United Nations specialized agency for information and communication | |

| Committee Acronym | Committee name | Description | Collaboration with SMESEC partner(s) |
|---|---|---|---|
| | Union | technologies – ICTs. The main products of ITU-T are Recommendations (ITU-T Recs) - standards defining how telecommunication networks operate and interwork. SG17: study group on security: standardises network and information security where numerous ITU-T recommendations have been developed including the security recommendations under the ITU-T X-series. | |
| OMA | Open Mobile Alliance | OMA is a non-profit organization that delivers open specifications for creating interoperable services that work across all geographical boundaries, on any bearer network. OMA's specifications support the billions of new and existing terminals across a variety of wireless networks, including traditional cellular operator networks and emerging networks supporting machine-to-machine device communications for the Internet of Things (IoT). | |
| OASC | Open & Agile Smart Cities | Open & Agile Smart Cities (OASC) is a global initiative connecting cities, advocating de facto standards, and sharing best practices. | |
| IETF | The Internet Engineering Task Force | The mission of the IETF is to make the Internet work better by producing high quality, relevant technical documents that influence the way people design, use, and manage the Internet. | UU, UOP |
| W3C | The World Wide Web Consortium | W3C is an international community where Member organizations, a full-time staff, and the public, work together to develop Web standards. W3C has recently launched the Web of Things Working Group to develop initial standards for the Web of Things, tasked with the goal to counter the fragmentation of the IoT; reduce the costs | |

| Committee Acronym | Committee name | Description | Collaboration with SMESEC partner(s) |
|---|---|---|---|
| | | of development; lessen the risks to both investors and customers; and encourage exponential growth in the market for IoT devices and services. | |
| IEEE-SA | Standards Association | IEEE has standardization activities in the network and information security space, and in anti-malware technologies, including in the encryption, fixed and removable storage, and hard copy devices areas, as well as applications of these technologies in smart grids. | |
| FIRST | Forum Of Incident Response and security Teams | FIRST is the premier organization and recognized global leader in incident response. Membership in FIRST enables incident response teams to more effectively respond to security incidents reactive as well as proactive. FIRST brings together a variety of computer security incident response teams from government, commercial, and educational organizations. FIRST aims to foster cooperation and coordination in incident prevention, to stimulate rapid reaction to incidents, and to promote information sharing among members and the community at large. | FORTH |

**Table 26: Longlist of available standardization bodies in the field of information and cybersecurity.**

Below we list relevant security standards which are published by the standardization bodies above, as relevant to the Standardization activities in SMESEC, by focusing on the areas related to our four pilot SMEs: Cyber Security, IoT, Smart Grids, Smart Cities, and E-voting.

#### 5.4.1.2.1 Cybersecurity

Regarding cybersecurity, ETSI has published many standards already, as shown in the following table.

| Standard | Standard title |
|---|---|
| TR 103 456 | CYBER; Implementation of the Network and Information Security (NIS) Directive |
| TS 102 165-1 | CYBER; Methods and protocols; Part 1: Method and pro forma for Threat, Vulnerability, Risk Analysis (TVRA) |
| TR 103 421 | CYBER; Network Gateway Cyber Defence |
| TR 103 306 | CYBER; Global Cyber Security Ecosystem |
| TS 103 307 | CYBER; Security Aspects for LI and RD Interfaces |
| TR 103 305-1 | CYBER; Critical Security Controls for Effective Cyber Defence; Part 1: The Critical Security Controls |
| TR 103 305-2 | CYBER; Critical Security Controls for Effective Cyber Defence; Part 2: Measurement and auditing |
| TR 103 305-3 | CYBER; Critical Security Controls for Effective Cyber Defence; Part 3: Service Sector Implementations |
| TR 103 305-4 | CYBER; Critical Security Controls for Effective Cyber Defence; Part 4: Facilitation Mechanisms |
| TR 103 331 | CYBER; Structured threat information sharing |
| TR 103 304 | CYBER; Personally Identifiable Information (PII) Protection in mobile and cloud services |
| TR 103 369 | CYBER; Design requirements ecosystem |
| EG 203 310 | CYBER; Quantum Computing Impact on security of ICT Systems; Recommendations on Business Continuity and Algorithm Selection |
| TS 103 307 | CYBER; Security Aspects for LI and RD Interfaces |
| TR 103 303 | CYBER; Protection measures for ICT in the context of Critical Infrastructure |
| TS 103 487 | CYBER; Baseline security requirements regarding sensitive functions for NFV and related platforms |
| TR 103 308 | CYBER; Security baseline regarding LI and RD for NFV and related platforms |
| TR 103 306 | CYBER; Global Cyber Security Ecosystem |
| TR 103 309 | CYBER; Secure by Default - platform security technology |
| TR 103 305 | CYBER; Critical Security Controls for Effective Cyber Defence |

**Table 27: Overview of ETSI standards on cybersecurity**

#### 5.4.1.2.2 IoT

Regarding internet of things, ETSI has published many standards as well, as shown in Table 28.

oneM2M has published its Release 2 in August 2016. The first oneM2M release includes specifications covering requirements, architecture, protocols, security, and management, abstraction

and semantics and Release 2 added new functionality, particularly by expanding management, abstraction and semantics. Specifications published by oneM2M can be accessed at: http://www.onem2m.org/technical/published-documents.

The IEEE Standards Association (IEEE-SA) has created a working group to develop its standard for an architectural framework for the IoT (P2413). In addition, IEEE has a number of existing standards, projects in development, activities, and events that are directly related to creating the environment needed for a vibrant IoT, recognizing the value of the IoT to industry and the benefits this technology innovation brings to the public: http://standards.ieee.org/develop/msp/iot.pdf.

The IETF (The Internet Engineering Task Force) has a number of working groups working on IoT. Security aspects of the IoT are being addressed in the following WGs: ACE and DICE. The Authentication and Authorization for Constrained Environments (ACE) WG (https://tools.ietf.org/wg/ace/charters) is working on a standardized solution for authentication and authorization to enable authorized access to resources on a device in constrained environments. In such environments, typical for the IoT, the network nodes are limited in CPU, memory and power. This work is supported by the recently chartered COSE WG that is building simplified CBOR analogues for the JSON object signing and encryption methods that were developed in the JOSE WG.

The DTLS In Constrained Environments (DICE) WG (https://tools.ietf.org/wg/dice/charters ) focuses on supporting the use of DTLS transport-layer security in these environments. Such constrained environments, including constrained devices (e.g. memory, algorithm choices) and constrained networks (e.g. PDU sizes, packet loss) are typical for the IoT, Smart grids, etc.

| Standard | Standard title |
|---|---|
| TR 103 422 | Digital Enhanced Cordless Telecommunications (DECT); DECT evolution technical study; Requirements and technical analysis for the further evolution of DECT and DECT ULE |
| GR IP6 008 | IPv6-based Internet of Things Deployment of IPv6-based Internet of Things |
| GR IP6 001 | IPv6 Deployment in the Enterprise |
| TS 118 122 | oneM2M Field Device Configuration (oneM2M TS-0022 version 2.0.0 Release 2) |
| GS NGP 001 | Next Generation Protocol (NGP); Scenario Definitions |
| GS NGP 005 | Next Generation Protocol (NGP); Next Generation Protocol Requirements |
| TS 103 268-1 | SmartM2M; Smart Appliances Ontology and Communication Framework Testing; Part 1: Testing methodology |
| TS 103 268-2 | SmartM2M; Smart Appliances Ontology and Communication Framework Testing; Part 2: Protocol Implementation Conformance Statement (PICS) pro forma |
| TS 103 268-3 | SmartM2M; Smart Appliances Ontology and Communication Framework Testing; Part 3: Test Suite Structure and Test Purposes (TSS & TP) |
| TS 103 268-4 | SmartM2M; Smart Appliances Ontology and Communication Framework Testing; Part 4: Abstract Test Suite (ATS) and Protocol Implementation eXtra Information for Testing (PIXIT) |
| TS 103 264 | SmartM2M; Smart Appliances; Reference Ontology and oneM2M Mapping |
| TR 103 435 | System Reference document (SRdoc); Short Range Devices (SRD); Technical characteristics for Ultra Narrow Band (UNB) SRDs operating in the UHF spectrum below 1 GHz |
| TR 103 411 | SmartM2M; Smart Appliances; SAREF extension investigation |
| TS 103 410-1 | SmartM2M; Smart Appliances Extension to SAREF; Part 1: Energy Domain |
| TS 103 410-2 | SmartM2M; Smart Appliances Extension to SAREF; Part 2: Environment Domain |
| TS 103 410-3 | SmartM2M; Smart Appliances Extension to SAREF; Part 3: Building Domain |
| TR 103 376 | SmartM2M; IoT LSP use cases and standards gaps |
| TR 103 375 | SmartM2M; IoT Standards landscape and future evolutions |
| TS 118 104 | oneM2M; Service Layer Core Protocol Specification (oneM2M TS-0004 version 2.7.1 Release 2) |
| TS 118 101 | oneM2M; Functional Architecture (oneM2M TS-0001 version 2.10.0 Release 2) |

**Table 28 : Overview on ETSI standards on Internet of Things**

#### 5.4.1.2.3 Smart Cities

Regarding smart cities, ETSI has published the following standards, shown in Table 29.

| Standard | Standard title |
|---|---|
| GS OEU 019 | Operational energy Efficiency for Users (OEU); KPIs for Smart Cities |
| TR 103 290 | Machine-to-Machine communications (M2M); Impact of Smart City Activity on IoT Environment |

**Table 29: Overview of ETSI standards on smart cities.**

#### 5.4.1.2.4 Smart Grids

IEEE has many standards and standards projects in development from the diverse fields of digital information and controls technology, networking, security, reliability, assessment, interconnection of distributed resources including renewable energy sources to the grid, sensors, electric metering, and broadband over power line, and systems engineering. IEEE has developed a guide for smart grid interoperability standardization, IEEE 2030-2011 IEEE Guide for Smart Grid Interoperability of Energy Technology and Information Technology Operation with the Electric Power System (EPS), End-Use Applications, and Loads. IEEE 2030(r) spans the three distinct perspectives of power and energy, communications and information technology: http://standards.ieee.org/develop/msp/smartgrid.pdf

The ITU smart grid focus group completed its work in December 2011 and adopted deliverables at http://itu.int/en/ITU-T/focusgroups/smart. The work was taken over by ITU-T SG15, which leads and coordinates this issue within ITU and with other organizations. ITU-T SG15 developed standards on power line communication (PLC, Recommendation ITU-T G.990x-series), which is one of the most important technologies for smart grids. ITU-T SG13 Recommendation ITU-T Y.2070 “Requirements and architecture of the home energy management system and home network services”, and consented Y.2071 “Framework of micro energy grid”. Detailed information is described in the document “smart grid standardization overview and work plan” developed by ITU-T SG15 and available at http://www.itu.int/en/ITU-T/studygroups/2013-2016/15/Pages/exec-sum.aspx.

### 5.4.2 ANALYSE phase: M7-M12

During this phase, all design aspects will be executed to enable the envisioned Federative Information Security Assessment engine, i.e. “the SMESEC maturity model”. It aims to provide an encompassing and easily maintainable artefact context for SMESEC’s partner technology stack and future developments in cybersecurity. ISO/IEC recognizes a distinct relationship between cyber-security and other security-related domains. The relationship between these security domains and cyber-security is depicted in Figure 31.

In parallel, we engineer the exact requirements for the envisioned SMESEC maturity model. A few examples of key requirements of the SMESEC model are provided here to illustrate our ambition

level. The assessment model needs to be developed on an architecture that allows for transparent standards lineage, i.e. for each capability in each focus area the underlying standard(s) need to be retrievable at will. Also, our aim is to operationalize each capability in each focus area with pragmatic implementation technology guidelines, based on the SMESEC technology stack where applicable. Finally, we address a major maturity model limitation in general, i.e. its mandatory manual expert tweaking in configuring the interdependencies throughout the model, which makes adaptations to ever-changing standards unmaintainable. We will build upon previous experiments using Rule-Based Management Systems (RBMS) and Graph-based Recommendation Systems to develop an architecture that invites maintainability-by-design. Figure 32 provides a first impression of a possible focus area structure of the SMESEC model.

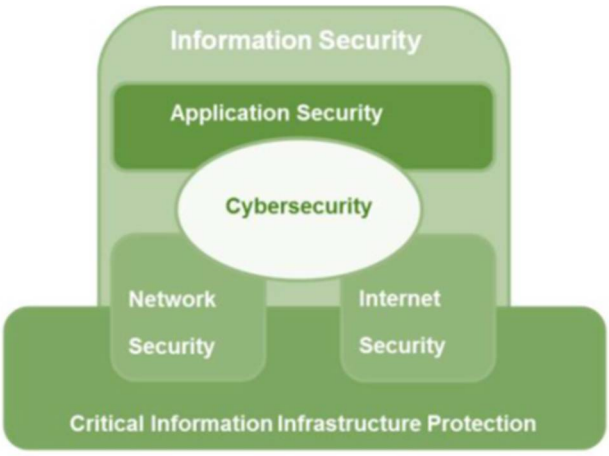


**Figure 31: Interdependent areas in Cybersecurity according to ISO27032.**

These two steps above result in a shortlist of security standards most relevant for SMESEC. We will contact these key standardization bodies to discuss collaboration opportunities and thus to build trust and a Security Standards Network, which will help propagate the SMESEC outcomes when they become available in SMESEC year 3.

| Focus Areas | Maturity Levels | | | | |
|---|---|---|---|---|---|
| **Cyber Security Maturity Model** | A | B | C | D | E |
| ***Organizational and Technical*** | | | | | |
| Server Protection | | | | | |
| End-user Controls | | | | | |
| Social Engineering Controls | | | | | |
| Network Security | | | | | |
| Application Security | | | | | |
| Cryptography | | | | | |
| Mobile Security | | | | | |
| Vulnerability Management | | | | | |
| ***Organizational*** | | | | | |
| Cyber Security Incident Management | | | | | |
| Cyber Security Awareness | | | | | |
| Cyber Security Governance | | | | | |

**Figure 32: First impression of the envisioned encompassing SMESEC model.**

### 5.4.3 DESIGN phase: M10-M18

In the overlapping DESIGN phase from M10-M18 we select the standards to integrate with the SMESEC framework, and formulate the extent to which SMESEC should support the standards. At

the same time, we develop a technical specification for the system implementation plan to more efficiently and effectively prototype the maturity model adhering to the specified requirements.

### 5.4.4 IMPLEMENT phase: M13-M24

In the IMPLEMENT phase from M13-M24 we implement the technical specification to more efficiently and effectively prototype the model iterations while adhering to the specified requirements. The resulting prototype integrates and enriches the original UU/SMESEC maturity models with the standards shortlist in a transparent and sustainable manner, while associating the available SMESEC technologies from all SMESEC partners with the appropriate maturity model capabilities. Note that piloting the model will already be possible at this stage using a paper-based version of the assessment. However, a flexible and maintainable analytic system implementation of the encompassing SMESEC maturity model is considered crucial for a long-lasting SMESEC impact.

### 5.4.5 EVALUATE & DEPLOY phase: M25-36

In the EVALUATE & DEPLOY phase in M25-36 we evaluate the final SMESEC model in our four case studies and possibly other environments to fine-tune its many aspects as appropriate. After a satisfactory evaluation, we will start positioning the SMESEC framework including the SMESEC maturity model as a unified meta-standardization framework for Cybersecurity in esp. SMEs, that we expect to be received well by all stakeholders due to its transparent meta-standards design, associated toolkit to help implement the personalized security advices, and the support of the standardization collaborators which we already contacted in Phase 2.

# 6 Conclusions

The preliminary market analysis on this document aims to establish the current market environment where the project is positioned. This initial analysis covers from the current trends, initial market segmentation and identification of market barriers, to an initial survey of the existing technologies and potential competitors. This initial work served as strong basis for building relevant dissemination and standardization project plans identifying respective SMEs target groups and appropriate SDOs combining a multi-dimensional approach based on market technologies and vertical pilots.

As part of the business model, the market will be monitored on a regular basis during the project lifespan and will be updated with any new relevant outcome that may have an impact on the project exploitation strategy. To maximize the project impacts, this close connection will be maintained all along the project with a set of communication measures to ensure the project visibility and the proper adoption of the SMESEC outcomes, strengthened by active contributions in standardization.

Since the technical results are still in a preliminary stage, the objective is to provide a reference to ensure that the technical dimension is oriented to the future market opportunities and to prepare an effective transfer to the market as soon as the project is finalized. The consortium will continuously update its strategy, presented in a dedicated set of deliverables with annual reports on exploitation, dissemination and standardization (M12, M24, M36). All this will provide a mature final version of the analysis included in the D6.5 Business model definition, due by M34.

# 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=EAIaIQobChMIwKbYl4D_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-vkMKY1wIVwZ0bCh21EQCxEAAYASAAEgLQrvD_BwE, retrieved date 2017-11-14

[16] Markets and Markets, Market-Reports https://www.marketsandmarkets.com/Market-Reports/user-entity-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=EAIaIQobChMIsYj6uqLS1wIV7hDTCh39qATuEAAYASAAEgIM9_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=EAIaIQobChMIiJ7W6aPS1wIVUhobCh3MTgNsEAAYAiAAEgIouvD_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 2017http://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, 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