SUCCESS

D6.6 v1.0

Report on Standardisation and Policies, V3

The research leading to these results has received funding from the European Union's Horizon 2020 Research and Innovation Programme, under Grant Agreement no 700416.

Project Name	SUCCESS
Contractual Delivery Date:	31.10.2018
Actual Delivery Date:	31.10.2018
Contributors:	P3C
Workpackage:	WP6 – Creating impact with SUCCESS
Security:	PU
Nature:	R
Version:	v1.0
Total number of pages:	30

Abstract:

In the context of Smart Metering and security, standardisation and dissemination in the respective user associations is paramount for the adoption of the SUCCESS results. SUCCESS has identified a significant number of relevant bodies and associations which focus on relevant areas. This deliverable presents the works regarding the discussions on adapting and focusing the content contributed to the standardisation organisations.

Keyword list:

Standardisation organisations, Smart Metering, Real time, security, Impact, Dissemination

Executive Summary

The SUCCESS project identifies standardisation contributions as a significant activity to ensure that the results are being used. In the context of Critical Infrastructures with high infiltration of smart devices, Smart Metering in particular and security in general, standardisation and dissemination in the respective user associations is paramount for the adoption of the SUCCESS results – real time secure Smart Metering whether in terms of software, hardware or processes and architecture, whether from the point of view of Information Technology (IT), communications or electrical components.

SUCCESS has identified a significant number of relevant bodies and associations which address areas relevant with the work and results of SUCCESS.

Towards reconfirming the selection of the appropriate bodies to disseminate the matching results, SUCCESS has taken up the task of standardisation since the beginning of the project. The SUCCESS partners have actively participated in meetings of standardisation bodies and user associations, holding presentations and making contributions, in cases when the relevant project results were mature enough. The process of standardisation is continuous and as such it was addressed by SUCCESS by an iterative process of examination of the match between requirements, maturity of results and initiated actions/contributions. This deliverable provides an overview of the considered bodies and the respective contributions. Contributions were done in form of presentations and discussions with the experts in the respective bodies with the content focus ranging from overall project achievements to specific SUCCESS results. In addition, one Work Item (WI) relating to the NORM and the ABCD Defender concept was approved and is running at the time of writing.

Furthermore, throughout the project duration, SUCCESS reached out to different authorities and organizations that could be interested to be specifically involved in a future operation of a Critical Infrastructure Security Analytics Network (CI-SAN). This deliverable presents the contacts and the associated feedback where such was given explicitly.

Authors

Partner	Name	e-mail
P3 COMMUNICATIONS GMBH (P3C)		
	Panagiotis	
	Paschalidis	panagiotis.paschalidis@p3-group.com
ISTITUTO SUPERIORE MARIO BOELLA SULLE TECNOLOGIE DELL'INFORMAZIONE E DELLE TELECOMUNICAZIONI (ISMB)		
	Mikhail	
	Simonov	simonov@ismb.it
ERICSSON GMBH (EDD)		
	Frank	
	Sell	frank.sell@ericsson.com
	Dhruvin Patel	dhruvin.patel@ericsson.com
OY L M ERICSSON AB (LMF)		
	Patrik	
	Salmela	patrik.salmela@ericsson.com
ENGINEERING – INGEGNERIA INFORMATICA SPA (ENG)		
	Antonello	
	Corsi	antonello.corsi@eng.it
SYNELIXIS LYSEIS PLIROFORIKIS AUTOMATISMOU & TILEPIKOINONION MONOPROSOPI EPE (SYN)		
	Theodore	
	Zahariadis	zahariad@synelixis.com
KEMA NEDERLAND BV (DNV GL)		
	Rooktabir Nandan	
	Sauba	ganesh.sauba@dnvgl.com

Table of Contents

1. Introduction

This document contains a description of the activities and contributions of the SUCCESS partners in relevant standardisation organisations. SUCCESS pursued active participation in standardisation meetings with the intention to promote its work towards specifying and standardising interfaces, Application Programming Interfaces (APIs), and gateways to achieve secure, seamless and interoperable communications and operation within and between elements in networks of Critical Infrastructures (CIs).

This is the final version of the document, deprecating all previous versions of the deliverable.

1.1 Scope of this Deliverable

The vulnerability of critical infrastructures through cyber-attacks using smart meters poses an extreme risk. The SUCCESS project deals with the improved security in CIs by investigating the contribution brought by smart meters and/or by other real time observational devices/sensors involved in Smart Metering processes. Among the new smart metering functionalities there is a real time sensing modality associated with real time control operations that could introduce new vulnerabilities.

The SUCCESS project delivered a new framework that includes among others:

- New-generation Open Real-time smart Meter (NORM) devices
- Critical Infrastructure Security Operation Centre (CI-SOC) that analyses NORM data, detects attacks and applies countermeasures to the detected threats
- a Breakout Gateway (BR-GW) infrastructure that facilitates the secure and efficient communication between the NORMs and the CI-SOC
- a Critical Infrastructure Security Analytics Network (CI-SAN) aggregating data from all utilities and external sources and detecting attacks on a pan-European level
- and new algorithms designed ad hoc to solve specific business issues

These components require interoperability with pre-existing and new elements of CIs. Interoperability is thus an important aspect, which is associated with standardisation activities. The effectiveness of the security features of the components regarding protection against and detection of any (cyber) attacks needs to be ensured before deployment. The expected interoperability and the requirement for a minimum guarantee of the security features call for standardisation actions.

In SUCCESS, contribution in standardisation and policies is perceived as an important outcome of the project. Although some existing standards have been deemed applicable for the SUCCESS components, they may not address all their aspects and features. Standardisation actions are, therefore, important in order to complement gaps in current standards.

Specifically, NORM will be built using a core functionality started in the Nobel Grid project [1], which will have basic implementations of standardised communication protocols such as Device Language Message Specification/COmpanion Specification for Energy Metering (DLMS/COSEM), IEC61850 and Message Queuing Telemetry Transport (MQTT). NORM has, however, new targets related to higher security (Physically Unclonable Function (PUF) technology) and Phasor Measurement Unit (PMU) integration. Making real-time Smart Metering interoperable with Smart Grid control operations implies addressing PMU specific communication protocols such as IEEE C37.118.1-2011 for Phasor Measurement Units and IEEE C37.244-2013 for Phasor Domain Concentrators (PDU). Those will be directly used or will be updated/changed in order to keep proper functionality or to offer new required functionality, such as Internet Protocol (IP) based time synchronization or other requests.

Additionally, SUCCESS has investigated and researched a solution to protect the real-time smart meters. In this context ISMB has evaluated existing industrialized solutions such as the Lockheed Martin Industrial Defender. Based on this evaluation, SUCCESS has decided to transform the research product (new algorithms) into the proof of concept “ABCD Defender” as described in the papers [2] and [3] and into a commercial product afterwards. For this reason, SUCCESS believes that the project standardisation actions are very important and is acting in the context described above. In order to influence standardisation (standardisation major actors are present at CEN, CENELEC, ETSI meetings, but not only, they are present at the Institute of Electrical and Electronics Engineers (IEEE) conferences and during events and fairs), ISMB decided to present their challenge, and namely the product concept ABCD Defender, during both major IEEE

Conferences (such as the SUCCESS workshop at Innovative Smart Grid Technologies (ISGT) and work in progress chair during the Event-Based Control, Communication and Signal Processing (EBCCSP) conference, trade fair in Brussels, the major Power and Energy Society (PES) conference in the United States of America (USA)), and during events at standardisation bodies (CEN, CENELEC, ETSI), and by challenging directly policy-making actors (mainly the European Commission and the JRC).

Existing standards can be related to other SUCCESS components as well. The BR-GW is related to 3GPP standards. Several features of USMC and ESMM could be standardised according to the IEC 62443 or International Organization for Standardization (ISO)/IEC 15408. More details with information of applicable standards are included in Deliverable D6.8 [4]. These standards may be able to be used as is, or modifications and updates may be required.

With these targets, SUCCESS has focused on these areas in order to assess what exists, to find the gaps and to propose new aspects for the standardisation, based on the experience incrementally obtained in the project.

1.2 Relationship to the work of the project

The current deliverable presents the work of SUCCESS towards communicating and establishing the aforementioned developed project results. Within this deliverable, only the minimal technical description is provided towards enabling the reader to comprehend the common and relevant topics of the respective bodies and organisations with the project results. For elaborate technical descriptions of the project results, the reader is referred to the respective project deliverables.

1.3 How to read this document

This deliverable is a standalone document that deprecates V2 of this deliverable (D6.5 [5]). This document has no prerequisite deliverables in terms of understanding beyond a general overview of the project results. The reader is nevertheless advised to be aware of the focus and the suggested SUCCESS solutions in order to fully comprehend the reasoning behind the choice of bodies and organizations. The document should be read linearly.

The remainder of this document includes: an overview of the relevant identified Standard Developing Organizations (SDOs) (Section 1.4) and policy making institutions (Section 1.5), an overview of the activities of SUCCESS within the relevant identified SDOs (Chapter 2) and the policy making institutions (Chapter 3). Finally, the document presents an overview of potential future work (Chapter 4) and concludes (Chapter 5).

1.4 Overview of relevant standardization organisations

SUCCESS partners considered and, where relevant, provided contributions in the following standardisation organisations:

- ETSI TC-Cyber
- ETSI TC-M2M, oneM2M
- ETSI MEC
- IEC MEC
- 3GPP SA1
- 3GPP SA2
- 3GPP SA6 (critical communications)
- IEC CEN-CENELEC
- EOS (European Organisation for Security)
- EU Smart Grid Coordination Group
- CIGRE WG B5, B3, D2
- IEFT CORE
- IEFT Privacy and Security Program

- WELMEC
- Smart Meter G3 Association
- PRIME Association
- ESMIG
- METERS AND MORE
- Open Smart Grid Protocol, DLMS User Group
- European Network for Cyber Security

The contributing partners in these organisations are: P3C, ISMB, EDD, DNV GL, ENG, ESB, ASM, LMF and SYN.

During the project timeline, SUCCESS addressed the standardisation challenges by contacting the above-mentioned bodies, by informing them about the scientific findings concerning the security and cyber-vulnerability of Smart Metering and Grid Control Infrastructures and the needs of updates of standards. The dissemination plan for the scientific findings and the project results included:

- the active participation and contribution of SUCCESS partners in working groups of standardisation bodies and user associations of great relevance to SUCCESS;
- invitations to interested organisations (including organisations with broader relevance to SUCCESS) to join the dedicated cyber security webinar organised within the IEEE PES in 2018, as well as to visit the open day trial sites, that took place in 2018. At the moment of writing of this deliverable, the Irish trial Site Open Day is planed for the 28th November 2018.

1.5 Overview of relevant policy making organisations

Policies and policy making activities are inherently linked to the standardisation mandates. For this reason, the SUCCESS partners considered and attempted contributions in the European major policy making organisations:

- The European Commission, the main policy making body in Europe
- The Joint Research Centre, the host that provides research and other services to support the Policy Making Process at pan-European Level
- Inter-institutional Competence Centres
- The organizations influencing policy making process through lobbying activities, for example the Union of the Electricity Industry (aka EURELECTRIC), as the sector association which represents the common interests of the electricity industry at pan-European level.

During the project timeline, SUCCESS addressed the challenge by contacting the above-mentioned bodies, by informing them about the scientific findings concerning the security and cyber-vulnerability of Smart Metering and Grid Control Infrastructures in order to influence the Policy Making Process by providing the evidence-based support, information, and the data.

Furthermore, SUCCESS heeded feedback regarding its comprehensive security concept spanning from the smart meter (NORM) to a Europe-wide security solution (CI-SAN) and contacted relevant authorities and institutions at community, state and international level to discuss on possible operational sceonarios, to identify and evaluate potential stakeholders and to pave the way forward for the development towards an operational solution.

2. Standardisation organisations and respective contributions

This chapter describes any contributions made in the framework of general or specific meetings, including dedicated work items and any other contributions. Furthermore, each section describes the plans, aspirations, considerations and current assessment regarding the suitability of SUCCESS results and the working scope of the working groups.

2.1 ETSI TC-Cyber

The ETSI Cyber Security committee (TC-Cyber) is working closely with relevant stakeholders to develop standards to increase privacy and security for organisations and citizens across Europe.

The ETSI TC-Cyber working group has among others the following areas of activity according to its Terms of Reference [6]:

- Cyber Security
- Security of infrastructures, devices, services and protocols
- Security advice, guidance and operational security requirements to users, manufacturers and network and infrastructure operators

These areas are to some extent relevant to the SUCCESS activities. The common point is that both the TC-Cyber working group and the SUCCESS project are looking in particular at the security of (Smart Metering) infrastructures, (observational) devices, (metering) services and protocols, as well as grid-wide and pan-European security tools and techniques to ensure security.

Considerable efforts have been made in the preparation for a work item suggestion on cyber security aspects for unbundled smart meters [7]. The purposes of this work item suggestion are:

- To initiate a discussion on the concept of unbundling the smart meter functionalities, i.e. segregating the metrology and the business/"smart" logic of the smart meters;
- To introduce a second metrology unit (low cost PMU), which will facilitate the measurements integrity controls;
- To promote the security features, such as hardware authentication and encryption, Role Based Access Control and different security zones for each external actor that are included in the development of the NORM within SUCCESS.

The work item has been suggested and approved during the TC-Cyber meeting in June 2018.

Activities regarding the promotion of SUCCESS have been done in most meetings (#7 to #10 and #12 to #14) that have taken place since the beginning of the project.

Table 1 SUCCESS promotional activites and contributions at TC-Cyber meetings

Meeting	Contribution	Partner
TC-Cyber #7 (06/2016)	• Disclosure of SUCCESS launch. • Promotion of SUCCESS as a project and related aspects on cyber security in the energy sector. • Suggestion of presentation of SUCCESS in the upcoming meetings	P3C
TC-Cyber #8 (09/2016)	• Presentation of SUCCESS • Preparation for suggestion of work items.	P3C
TC-Cyber #9 (02/2017), **TC-Cyber #10 (05/2017),** **TC-Cyber #12 (02/2018)**	• Discussion with delegates towards building up support for new work item • Assessing interest in SUCCESS content	P3C

TC-Cyber#13 (06/2018)	• Presentation of the SUCCESS WI proposal P3C and ISMB. • Adoption of the WI form the ETSI Technical Board (TB)	ISMB, P3C
TC-Cyber#14 (10/2018)	• Presentation of the stable draft of the Technical Report during the ETSI meeting.	ISMB, P3C

In addition to the above, SUCCESS has undertaken consensus building actions by organising discussions about the SUCCESS context and smart metering solutions being developing with several ETSI partners (specifically Telecom Italia, Siemens, Orange, and ETSI secretariat). In order to step to the active standardisation stage, the consensus of at least three ETSI affiliates is required. SUCCESS activities and products have been promoted in bilateral meetings during major public events (conferences, fairs) and other events that have taken place since the beginning of the project.

Given the amount of the previously described activities, ETSI experts have agreed to accept the proposed work item. Consequently, ISMB partner was assigned a rapporteur role in guiding the progress of the above mentioned Draft Technical Report (DTR)/Cyber-0037 work item [7]. In the Technical Report the guidelines for increasing smart meter security based on the outcomes of SUCCESS are included.

As a result, the inclusion of SUCCESS-specific topic in the TC-Cyber agenda is a significant achievement being already consolidated, while the follow up is considered for one of next meetings in Sophia Antipolis (France) and the publication is foreseen in April 2019.

The current roadmap of the work item [7], annotated as the ETSI TR 103 644 is presented in Figure 1.

Details of 'DTR/CYBER-0037' Work Item Schedule

Code	Status	Milestone	Action	Action Nb	Target	Achieved	Version
0	Creation of WI by WG/TB	Creation of WI by WG/TB			2018-06-06	2018-06-06	
0 p	WI proposed to TB	WI proposed to TB				2018-06-07	
0 a	TB adoption of WI	TB adoption of WI			2018-06-08	2018-06-07	
1	Start of work	Start of work			2018-06-08	2018-06-08	
2	Early draft	Early draft					
4	Stable draft	Stable draft			2018-10-05	2018-09-26	0.0.1
4	Stable draft	Stable draft				2018-10-05	0.0.2
6	Final draft for approval	Final draft for approval					
8	TB approval	TB approval			2019-02-22		
8 A	Draft receipt by ETSI Secretariat	Draft receipt by ETSI Secretariat			2019-03-08		
12	Publication	Publication	PU		2019-04-05		1.1.1

Figure 1: Current roadmap of the SUCCESS work item at the ETSI TC-Cyber

2.2 ETSI TC-M2M, OneM2M

The ETSI TC-Machine to Machine (TC-M2M) working group has among others, the following relevant areas of activity according to its Terms of Reference [8]:

- M2M Quality of Service (QoS) considerations
- M2M Security and Privacy

Furthermore, the purpose of the related oneM2M group is to develop technical specifications which address the need for a common M2M Service Layer. The group has also the following areas of activity [9]:

- Common use cases, terminal/module aspects, including Service Layer interfaces/APIs between a) Application and Service Layers, b) Service Layer and communication functions
- Security and privacy aspects (authentication, encryption, integrity verification)
- Information models and data management (including store and subscribe/notify functionality)
- Architecture – functional entities, reference points, and related message flows
- Interworking aspects (e.g. leveraging network capabilities as and when applicable)

In that, the SUCCESS results are potentially relevant for the Architecture and Security work groups. Some of the anticipated implications do not seem to be as relevant for OneM2M, as the vertical specific aspects have been lowered in focus, which means that there is a focus on generic and vertical independent architectures and solutions. Throughout the duration of the project, no requirements and architecture gaps related to the SUCCESS security architecture and the NORM specification were identified that could be brought forward to the OneM2M (or if relevant to ETSI TC-M2M).

2.3 ETSI Smart Metering

ETSI Smart Metering is a body that collaborates with the European Committee for Standardisation (CEN) and the European Committee for Electrical Standardisation (CENELEC) in response to the European Commission Mandate M/441 on Smart Metering. This Group contributes to the development of Smart Metering, to the standardisation of Machine-to-Machine communications, and the development of an application-independent 'horizontal' service platform capable of supporting a wide range of services including Smart Metering, Smart Metering use cases, and the security of smart energy infrastructures.

SUCCESS contributes directly in the Smart Metering scenario because of the real time smart meters, NORMs, event-based meters, and low cost PMUs. For this reason, we have contacted this Expert Group.

Table 2 SUCCESS promotional activities at ETSI Smart Metering meeting

Meeting	Contribution	Partner
27/09/2016 (09:30-11:00) in conjunction with the ICT Proposer Day	• Information about the SUCCESS objectives and activities. • Promotion of SUCCESS as a relevant project dealing with cyber security aspects. • Suggestion of presentation of SUCCESS in the upcoming meetings	ISMB

2.4 ETSI STF 516 Standardisation for EU Mandate M/462

The ETSI STF 516 Standardisation Expert Group operates for the implementation of the European Union (EU) Mandate M/462 that focuses on the ICT to enable efficient energy use in fixed and mobile information and communication networks. It deals with the critical infrastructures that will embed real time Smart Metering in these networks. For this reason, we decided to raise the awareness in the STF 516 Expert Group about the SUCCESS and the related developments.

SUCCESS directly contributes in a more efficient energy use by offering real time smart meters feeding real time control operations. In effect, NORMs, event-based meters, and low cost PMUs are valuable data sources that will provide the background for real time optimization and decision making about a more efficient energy use. For this reason, we have contacted this Expert Group.

Table 3 SUCCESS promotional activites and contributions at ETSI STF 516 meetings

Meeting	Contribution	Partner
13 September 2016 in ISPRA at JRC premises	• Role of the enabler of efficient energy use in fixed and mobile information and communication networks in the context of M/462 Standardisation Mandate • Information about the SUCCESS objectives and activities. • Promotion of SUCCESS as a relevant project dealing with cyber-security aspects.	ISMB
17 May 2017 at European Interoperability Centre for Electric Vehicles and Smart Grids	• Has been provided scientific input on the latest and most innovative methods of smart grid monitoring in the context of M/462 Standardisation Mandate • Information about the SUCCESS activities and outputs. • Challenging the adoption of SUCCESS outputs in the context of Smart Grid Interoperability Laboratory at the JRC sites.	ISMB

2.5 ETSI Mobile Edge Computing (MEC)

The ETSI MEC initiative is an industry specification group within ETSI. The work of the MEC initiative aims to unify the telco and IT-cloud worlds, providing IT and cloud-computing capabilities within the Radio Access Network (RAN) [10], notably part of a mobile telecommunication infrastructure.

The plans of SUCCESS regarding this initiative was to achieve an alignment of the activities regarding double virtualization and NFVs on top of power grids.

However, after reviewing the scope of the planned activities of SUCCESS and considering the scope of ETSI MEC, the curent project judgement assumption is that there is no overlap between SUCCESS project results and the work of the ETSI MEC group. The focus of the SUCCESS work is to execute Smart Metering functions in an intelligent distributed cloud, bringing core network capabilities closer to the access points, while the MEC standardisation focuses on implications and impacts on radio equipment induced by the integration of edge cloud capabilities. Monitoring of the MEC standardisation continued through the project, but no relevant aspects were encountered.

2.6 3GPP SA1

In the context of the SUCCESS project activities, 3GPP Service and System Aspects (SA) number 1 standardisation group [11] activities were investigated. 3GPP SA1 suggests and analyses requirements; in particular, the study item “5G communication for Automation in Vertical domains” identifies the requirements on the 5G communication systems for different vertical domains including security aspects. Requirements include topics such as availability, reliability and security, and were described for each use case. During the duration of the project, not enough common ground was found for an explicit contribution.

2.7 3GPP SA2

In the context of the SUCCESS project activities, 3GPP SA2 standardisation group [12] activities were investigated. In Release 14, specification of the CUPS (Control and User Plane Separation of the Evolved Packet Core (EPC) nodes) [13] was introduced. This allows for more flexible and distributed deployment of the control and user plane functions. The result is reduction of the latency on application services when realized near the RAN. The CUPS also allows to enable Software-Defined Networking (SDN) to deliver the user plane functionality more efficiently. This architecture will allow the realization of distributed countermeasure implementation developed in the SUCCESS project. During the duration of the project, not enough common ground was found for an explicit contribution.

2.8 3GPP SA6 (critical communications)

SA6 is responsible for the definition, evolution and maintenance of technical specification(s) for application layer functional elements and interfaces supporting critical communications, including relevant application architectural aspects (including both network and terminal aspects) [14].

The current focus of the SA6 work group is around mission critical video and communication services (such as push to talk). Contributions in SA6 were considered for other mission critical data communication services, which relate to mission critical services with respect to the detection or mitigation of security threats, but in the end were not carried out.

2.9 CENELEC TC215

The Smart Metering functionality is part of the Cyber-Physical System that includes electrical and telecommunication aspects. For this reason, this functionality is relevant to the activities performed by the CENELEC TC 215 expert Group focused on the electrical aspects of telecommunication equipment. In a real-time control scenario, smart meters heavily use telecommunication equipment, while industrial applications use Smart Metering in order to improve energy efficiency.

The SUCCESS project was built upon the interoperability between real time smart meters and the Automatic Meter Reading (AMR) / Advanced Metering Infrastructure (AMI) / Supervisory Control and Data Acquisition (SCADA) implemented during the FINESCE project [15]. The SUCCESS project implemented a pan-European Security service that uses telecommunication equipment. The set of electronic devices making part of the SUCCESS framework, such as NORMs, event-based meters, and low cost PMUs, will be part of the pan-European infrastructure that already raises electrical aspects of telecommunication equipment. This has led SUCCESS to contact this Expert Group.

The Intelligence Based Protection (concept developed by ISMB and initially presented during the EBCCSP 2017 conference) exploits the interoperability between SCADA and meter management, e.g. Advanced Meter Management (AMM) / AMR, systems. Since the interoperability is one of the aspects of standardisation (communication protocols) ISMB has chosen CEN, CENELEC, and ETSI as possible standardisation bodies to address this aspect.

Table 4 SUCCESS promotional activities and contirbutions at CENELEC meetings

Meeting	Contribution	Partner
13 September 2016 in - ISPRA at JRC premises	• Discussion about the electrical and telecommunication aspects of Smart Metering in real time scenario • Presentation of the event-based smart meter in SOA/EDA context of Future and Next Generation Internet • Information about the SUCCESS objectives and activities.	ISMB
8-9 May 2017 in Brussels at CEN CENELEC premises	• Has been provided scientific input on the SUCCESS approach to the use of	ISMB

And follow up (several contacts during June - October 2017)	real time smart metering functions in the context of green data centres. • Discussion about the needs for energy efficiency in resource demanding business scenario (High Power Computing). • Presentation of five possible scenarios of the use of SUCCESS outcomes in the standardisation context, after the current mandate. • Information about the SUCCESS outputs and specifically NORM, Agent-based security framework and the use of 5G technology.	
6 September 2017 in Brussels at CEN/CENELEC premises	• Presentation of SUCCESS project to the TC205 WG18 committee. • Discussion on how the outcome of SUCCESS could be adopted to the new Cybersecurity/SmartGrid WG that is being proposed.	DNV

SUCCESS intended to also contribute to the Smart Grid related groups by disseminating the outcomes from the trial operations, the evaluation of NORM requirements and design through the webinars and the trial site open days at a later point in time.

Given the ongoing work on the ETSI TR 103 644, the proactive actions vs. CEN/CENELEC are not in the main scope for the next period. After the completion of the ETSI TR 103 644, the final document will be disseminated to the CEN/CENELEC in the context of a coordinated standardization process.

2.10 CEN-CENELEC-ETSI Coordination Group on Smart Energy Grids (CG-SEG)

The CEN-CENELEC-ETSI Coordination Group on Smart Energy Grids (CG-SEG) was established in 2011 in response to the Smart Grid Mandate M/490 by the European Commission [16]. The work done by the CG-SEG was continued after the closing of the mandate M/490 with the purpose to follow-up on the standardization gaps identified during the first phase of M/490 and to provide best practice examples on smart energy grid specific use cases [16].

SUCCESS has contacted the coordination group disseminating relevant content. SUCCESS partner P3E was also invited to participate and present SUCCESS at the “Set of Standards” Working Group.

2.11 CIGRE WG B5, B3, D2

CIGRE is an international non-profit Association for promoting collaboration with experts from all around the world by sharing knowledge and joining forces to improve electric power systems of today and tomorrow [17]. CIGRE has the following SUCCESS relevant focus in the different Study Committees:

- Cyber security requirements for Smart Metering
- Requirements for the establishment of a pan-European security monitoring system
- Outcomes from trial operations and guidelines for cyber-physical security.

These topics are covered at different levels each within the Study Committees SC B5, B3 and D2, which were addressed during the progress of the project. SUCCESS has provided a contribution in the form of a scientific paper, which was unfortunately not accepted.

The Study committee B5 covers principles, design, applications, coordination, performance and asset management of [18]:

- System Protection
- Substation Control and Automation
- Remote Control Systems and Equipment
- Metering Systems and Equipment.

The focus is placed on design and application of digital technology and modern integrated system approach including hardware and software for the acquisition of system state information, local and remote data communication, and execution of control commands [18].

The Study Committee B3 is responsible for the design, construction, maintenance and ongoing management of substations and for electrical installation in power stations, excluding generators. Major objectives include increased reliability and availability, asset management, environmental impact containment, and the adoption of appropriate technological advances in equipment and systems to achieve these objectives [19].

Study Committee D2 (SC D2) covers the specification, design, engineering, performance, operation, maintenance, economic and management aspects of the Information and the Telecommunication systems in the Electricity Power Industry (EPI) both for operational and business activities, as well as the different devices, media and networks to support all that services: speech, data, video, internet, specialized signalling for teleprotection, SCADA, Energy Management Systems (EMS), Demand-Side-Management (DSM) [20]. Study Committee D2, which is of relevance to SUCCESS will coordinate, along with other Study Committees, these topics.

2.12 IETF

2.12.1 IETF CORE

In the SUCCESS project, topics such as secure bootstrapping and service discovery were set in the context of deployment of smart meters. Amongst others, the IETF has studied these topics in general. Currently, the Constrained RESTful Environments (CORE) WG is particularly active, with 4 documents sent to IESG review of which several other have resulted in RFCs (RFC8075, RFC8132, RFC8323 and RFC8428). CoAP over TCP is now an RFC being used in particular in NATed (Network Address Translation) environments. OSCORE (Object Security for Constrained RESTful Environments) is about to become an RFC too, providing another security mechanism independent of the transport layer. SenML is also an RFC now, providing a JavaScript Object Notation (JSON) like serialization for sensors. This work is also being delivered to the Open Mobile Aliance (OMA) for their Lightweight M2M (LWM2M) protocol.

The focus of the work in CORE is now moving to hypermedia and data representation, extending the Web Link format and adding new media types for various other SDOs. In the future, some work started in T2TRG might be moved on to CORE as it matures.

Contributions from the project partners may relate to enhancements to current IETF standards, or alternative or complementing solutions, as input to the IETF, and the CORE WG especially. Since the use cases of the SUCCESS project have a very concrete and specific focus, it might well be that these use cases with their own unique requirements introduce new features and requirements e.g. on secure bootstrapping and service discovery solutions, which might not have been considered in the generic solutions defined by the IETF. Introducing new features/solutions resulting from SUCCESS might happen after the project has been finalized as it is beneficial that standards are generic enough to fit multiple use cases. This requires that multiple verticals are analysed before a widely compatible solution is suggested.

2.12.2 IETF ACE

Authentication and Authorization for Constrained Environments (ACE) has been a key WG for Internet of Things (IoT) in IETF. It has developed several profiles for authentication in constrained environments that range from Datagram Transport Layer Security (DTLS) to Open Authorization (OAuth) and OSCORE. It has several documents in the last stages of standardization (ace-dtls-authorize, ace-oauth-oauthz, ace-oscore-profile). Ericsson has been and is still actively participating to the work.

2.12.3 IETF SUIT

The Software Updates for IoT (SUIT) working group is trying to standardize the metadata needed in order to secure the firmware update process. This is important especially for secure IoT deployments. When fetching firmware the device also fetches a signed manifest file. At boot time, the device compares the manifest to the actual firmware image before flashing.

SUIT has been very active in IETF hackathons and has only recently been chartered, thus the group has not yet produced any RFCs. However it is an important work that will be used by other SDOs like OMA.

2.12.4 IETF LWIG

The Light-Weight Implementation Guidance (LWIG) Working Group focuses on helping the implementors of constrained devices, which makes it relevant for IoT in general, including smart grids. The informational draft documenting implementation experiences of public-key cryptography on small devices was this year published as RFC 8387 [21]. The draft shows that it is often incorrectly assumed that resource-constrained IoT devices cannot perform cryptographic operations needed for strong security. The draft documents experiences of implementing Rivest, Shamir y Adleman (RSA) cryptosystem and Elliptic Curve Cryptography on small micro-controllers. Based on the continuous contributions and voluntary work, LMF has been appointed the co-chair of the LWIG working group.

2.12.5 IETF EMU

The Extensible Authentication Protocol (EAP) Method Update (EMU) working group has been chartered to provide updates to some commonly used EAP methods. The Extensible Authentication Protocol (EAP) [RFC 3748] is a commonly used network access authentication framework, which has also been adopted by the 3GPP for 5G. LMF has been instrumental in starting the EMU working group at the IETF. The working group charter was approved by the IESG in February 2018 and LMF was appointed as the co-chair in July 2018.

LMF has submitted a draft updating EAP-TLS given that we have a new version of TLS namely, version 1.3 [22]. This document will update RFC 5216 and is already adopted as a working group document.

LMF also has prepared a draft contribution for secure bootstrapping of IoT devices. This contribution would extend the EAP framework and define a method for out-of-band (OOB) authentication and key derivation [23]. This EAP method is intended for bootstrapping all kinds of IoT devices that have a minimal user interface and no pre-configured authentication credentials. LMF has been updating the open-source implementation of the EAP Nimble out-of-band authentication (EAP-NOOB) protocol [24] together with Aalto University. Additionally LMF is working on developing a formal model of the protocol to verify its correctness. LMF also has prepared two drafts on EAP-Authentication and Key Agreement (EAP-AKA') related enhancements that aim to align the EAP-AKA' method to the latest 5G specification [25] and add new features such as perfect forward secrecy [26].

2.12.6 IETF 6LO

The LMF contribution on secure neighbour discovery for resource-constrained devices was updated in February 2018 based on feedback received [27]. Since then, we have received many security related questions from the IETF community as well as the security area directors (Eric Rescorla and Benjamin Kaduk). We have been answering the questions received and are now in the process of updating the draft before the next IETF. This contribution defines an extension to existing neighbor discovery mechanism specified in RFC 6775 to provide additional security. Nodes supporting this extension would rely on cryptographic addresses instead of the Extended Unique Identifier 64 (EUI-64) addresses that are specified in RFC 6775. The working group has after discussions concluded that it would use 256-bit identifiers for addressing. While this would increase the cost of routing marginally, the resource-constrained nodes would not have to solve cryptographic puzzles for registering cryptographic addresses (which was the case for Cryptographically Generated Address (CGAs) defined in RFC 3972).

2.12.7 IETF T2TRG

The overview document on IoT security, which is part of the Thing-to-Thing Research Group (T2TRG) [28], has now been reviewed and voted on by the leadership of the IRSG (Internet Research Steering Group). Note that the document has already undergone 3 revisions since the

last report. The document will now be sent to the IESG for final checks before it is submitted to the RFC editor for publication. This document discusses the various stages in the lifecycle of an IoT device. It then documents the security threats to an IoT device and the challenges that one might face in order to protect against these threats. Lastly, it discusses the next steps needed to facilitate the deployment of secure IoT systems.

2.12.8 IETF Privacy and Security Program

The IAB (Internet Architecture Board) Privacy and Security Program is a small group of people discussing the topics of privacy and security in the Internet. The discussion procedure is different than many working groups in IETF. However, by following the focus of the group, SUCCESS could achieve a good insight into the group's view on current topics related to Internet privacy and security. The group also organises workshops and participation to relevant workshops of theirs were considered for discussing findings of the SUCCESS project. One high impact workshop arranged by them was the MaRNEW 2015 workshop [29].

2.13 WELMEC

WELMEC is a non-binding European cooperation in the field of legal metrology. Its Members are representative national authorities responsible for legal metrology in European Union and European Free Trade Association (EFTA) member states. WELMEC remains a free cooperation in which agreement is sought on a range of issues of mutual interest and wide importance and is effectively a widely accepted across Europe guide to best practice based on the Measuring Instruments Directive 2004/22/EC [30].

As regards Smart Metering and the relevance of SUCCESS results for WELMEC, the proper part of WELMEC guidelines are those specifically in Section 7.2 (Working Group 7) [31]. The guidelines structures are organised as a set of requirement blocks. The overall structure in fact follows the classification of measuring instruments into basic configurations and the classification of so-called IT configurations. The set of requirements is complemented by instrument-specific requirements [31]. SUCCESS aspired to disseminate the project results in this group, through the participation of WELMEC in the webinars and in the trial site open days.

2.14 Smart Meter G3 Association, PRIME Association, ESMIG, METERS AND MORE

Within large end-user associations such as ESMIG [32] and Meters And More [33], SUCCESS disseminated the outcomes from the trial operations and the evaluation of the NORM requirements and design. Willem Strabbing, Managing Director at ESMIG, was invited to join the Advisory Board of SUCCESS and became an Advisory Board member in order to assist in a strategic alignment of the project and to advance consensus on European certification approaches regarding security and interoperability in the domain of Smart Metering. Furthermore, Meters And More was contacted during the European Utility Week 2017 to establish a regular exchange regarding open protocols relevant for NORM.

2.15 Open Smart Grid Protocol, DLMS User Group

More specific user associations on cyber security and specific communication protocols such as the Open Smart Grid Protocol [34] and the DLMS user group [35] were considered by SUCCESS towards aligning, through their presence and participation in the webinar and the trial site open days, on the respective results from security testing activities on NORM and threat analysis on the relevant protocols.

2.16 European Network for Cyber Security

The European Network for Cyber Security is a non-profit member organisation that brings together critical infrastructure owners and security experts to address secure infrastructure with a distinct focus on smart energy grids [36]. As such, SUCCESS has contacted the European Network for Cyber Security (ENCS) towards disseminating results on the identification and modelling of new cyber threats as well as on cyber security certification.

2.17 JRC

Specifically, in June 2017 ISMB has presented to the JRC the SUCCESS risk modelling approach (part of the D1.4) in the view of the Climate Change Policy and the new Energy Directive. The project interacted with the newly created Competence Centre on Modelling in order to contribute in the modelling process and the repositories with the Use Cases, industrial best practice descriptions, and proposals for standardisation.

The Commission issued the document "Benchmarking smart metering deployment in the EU-27 with a focus on electricity", jointly drafted by the Dictorate-General for Energy (DG ENER) and JRC, as COM(2014)356. This report gauges progress in the deployment of intelligent metering in the EU Member States on the basis of economic assessments of the long-term Costs and Benefits Analysis (CBAs) of electricity and gas smart metering prepared by Member States and submitted to the Commission in line with Third Energy Package provisions. Based on the above data, interventions at the European Commission and the JRC premises are considered appropriate because these hosts challenge standardisation bodies by issuing the mandates for standardisation. An example of such mandates is the Mandate M/441 on Smart Metering. Inside the JRC, the Smart Grid Interoperability Centre exists and presents a networking opportunity to promote the adoption of SUCCESS outcomes. For this reason, SUCCESS informed the EC and the JRC about the standardisation of Machine-to-Machine communications, and the development of e-energy service platforms capable of supporting a wide range of services including Smart Metering, Smart Metering use cases, and the security of smart energy infrastructures.

The European Commission uses *modelling* to assess the environmental, economic, and social impacts of policy options and policy initiatives. Models are also used in other phases of the policy cycle, for instance to support implementation. The Commission's increasing focus on quantification of EU policy requires cross-cutting and robust approaches. Newly created Competence Centre on Modelling (officially inaugurated on 26th October 2017) brings under one umbrella the Commission's competencies and best practice in building and using models for greater quality and transparency in policy making.

The Competence Centres in the JRC are centred on analytical tools which can be applied to any policy area (Energy and Climate included), bringing together in one place extensive expertise in this field. They offer training courses in the use of the tools for policy-making, advise on the choice of tools and also work directly with the Commission Policy Directorates-General to apply the tools to the policy problems at hand. The Competence Centre on Modelling is the fourth one in the JRC, after the Competence Centres on Composite Indicators, Microeconomic Evaluation and Text Mining and Analysis. Given the focus of these organisations, SUCCESS had a unique opportunity to contribute, by informing about the SUCCESS cyber-risk modelling approach and by promoting the SUCCESS models and tools as candidates for the inclusion in the Modelling Inventory Database and Access Services (MIDAS) repository of models, to:

- the Commission's Better Regulation policy, to
- the Inter-Institutional Agreement on Better Law Making, and to
- the Communication on Data, Information and Knowledge Management at the European Commission.

The incorporation in the CC-MOD of one of the SUCCESS participants (list is available online [37]) presents a challenge to inform the policy making community and modellers about the cyber-risk approach to modelling being developing in SUCCESS.

2.18 CEN/CENELEC TC205/ZVEI

The work we have carried out in SUCCESS was presented to the CEN/CENELEC TC205 committee members and this was further reported to ZVEI (Zentralverband Elektrotechnik- und Elektronikindustrie e.V.). That's the German electrical and electronic manufacturers association which is one of the most important industrial associations in Germany. This initiative is trying to bring industry and Standards bodies to work closer together by creating a European Cybersecurity Union.

3. Work with Authorities with respect to policies and operational prospect for the CI-SAN

SUCCESS has organised events and meetings for authorities. The aim of these dissemination activities is the promotion of the concepts and project results to authorities, so that they foster the establishment of the SUCCESS architecture. The contribution of the SUCCESS components in the cyber security of critical infrastructures can persuade the respective decision makers at national or European level to regulate towards the implementation of the SUCCESS architecture.

The following sections showcase all dissemination activities that involved authorities as the main audience.

3.1 Whitepaper

SUCCESS published a whitepaper [38] in January 2018 entitled “A European Security Analytics Network for Critical Infrastructures”, which suggests how European authorities can be addressed by the SUCCESS consortium in order to regulate at a pan-European basis the establishment of the Critical Infrastructure Security Analytics Network (CI-SAN).

In summary, it is suggested that the Distributed System Operator (DSO) – members of the SUCCESS consortium, being themselves end users of the SUCCESS architecture, are most suitable to initiate discussions with authorities. The key message to convey to authorities is the necessity for a pan-European network that can perform data analytics on aggregated data from all critical infrastructures in Europe and can thus identify coordinated and cross-infrastructure attacks. The initial contacts of the DSOs can be politicians and agencies at regional or national level. Eventually, provided that the primary contact points continue to pass the need to higher levels, European decision-making committees can be reached bottom-up. Other European DSOs and critical infrastructure operators can also contribute thereto, by also addressing their own contacts in authorities regarding the promotion of the concept of CI-SAN.

3.2 European DGs

Within the European DGs, the Dictorate-General for Migration and Home Affairs (DG Home) and the Dictorate-General for Communications Networks, Content and Technology (DG CNECT) were identified beyond the home DG of the project. The relevance of DG CNECT is straightforward, since SUCCESS deals with cyber security for critical infrastructure with its use cases focused in the energy domain. The relevance of DG Home was pinpointed regarding the CI-SAN and the detection of security issues on a pan-European level. Terrorist attacks and cyber-warfare may well target critical infrastructure to achieve their goals.

SUCCESS has identified relevant contacts within the respective DGs and has disseminated relevant information.

3.3 TSCNET

TSCNET [39] is a Transmission System Operator (TSO) organisation based in Munich. Its targets include cooperation among the 13 members towards accomplishment of the system security. The aspiration of TSCNET is to develop the methods, processes and tools to meet the growing complexity of the European interconnected energy grid. TSCNET is one of the SUCCESS relevant customers of P3E, and as such SUCCESS content has been regularly discussed in meetings with it.

3.4 EE-ISAC

The European Energy – Information Sharing & Analysis Centre (EE-ISAC) [40] is an industry-driven, information sharing network, that is very similar to the CI-SAN concept. The EE-ISAC is the result of the European research project Distributed Energy Security Knowledge (DENSEK) [41], which was realized with the financial support of the Prevention, Preparedness and Consequence Management of Terrorism and other Security-related Risks Programme under DG Home. Using the EE-ISAC, its members can share real-time security data, reports on security incidents and breaches etc. SUCCESS and specifically P3E, has approached EE-ISAC as soon as a webpresense went online to exchange information and ideas regarding the two concepts.

EE-ISAC has signalled also the interest in the SUCCESS concepts and more specifically in the CI-SAN. P3E is invited to participate in the next regular meeting.

3.5 EDRi

European Digital Rights (EDRi) is an association of civil and human rights organisations from across Europe, with a view to defend rights and freedom in the digital environment [42]. EDRi is relevant for SUCCESS, also in terms of its privacy by design approach. EDRi was contacted by SUCCESS, but a more close exchange was postponed due to the current focus and load of the association on the implementation of the General Data Protection Regulation (GDPR) guideline.

3.6 Med-TSO

Med-TSO [43] is the Association of the Mediterranean TSOs for electricity, operating the High Voltage Transmission Networks of 19 Mediterranean countries. SUCCESS partner CRE is a member of Med-TSO. Med-TSO was established as a technical platform, that uses multilateral cooperation as a strategy of regional development [43]. As such Med-TSO is relevant for SUCCESS based on the cooperation and consensus needed towards establishing a real-time information sharing network. SUCCESS partners were invited and attended at the Mediterranean Project Closing Conference: “Towards the Future Secure and Sustainable Electricity Infrastructure in the Mediterranean Region” at European Parliament, on 10 April 2018.

3.7 ENTSO-E

The European Network of Transmission System Operators for Electricity (ENTSO-E) is a large TSO association with a key role in developing a pan-European grid and achieving the ambitious European decarbonization goals by 2050 [44]. As such, it is relevant for SUCCESS in terms of a forum where standards and systems for its member organizations are discussed and supported. ENTSO-E is one of the SUCCESS relevant customers of P3E, and as such SUCCESS content has been regularly discussed in meetings with it.

3.8 German Authorities

The SUCCESS partners have initiated discussions with German authorities regarding the feasibility of the SUCCESS architecture in Germany.

A meeting with the Federal Office for Information Security, i.e. Bundesamt für Sicherheit in der Informationstechnik, (BSI) [45] was organised therefor. The feedback focused on potential attack surfaces. More specifically, when introducing new systems and data access – for data sharing – new vulnerabilities may be introduced, so operators need to be very cautious when considering such systems. Small autarch regions with the minimum amount of outside connections can be safer than an unchecked information sharing system.

SUCCESS partners have met with the Cyber and Information Domain Service Headquarters (KdoCIR – Kommando Cyber- und Informationsraum) of the German Armed Forces [46] to present the project SUCCESS and to investigate possibilities and interest on CI-SAN. KdoCIR’s feedback is positive in terms of necessity for awareness on cyber threats as well as methods to detect and mitigate ongoing attacks. However, since CI-SAN mainly refers to civilian infrastructure, it cannot be directly considered as relevant for KdoCIR and the Armed Forces. Moreover, the Technical Readiness Level (TRL) of CI-SAN – as a result of a research and innovation project – is too low, to be considered as a complete, that is, operational, suggestion and thus evaluated as such. Various technical aspects and components need to be evaluated beyond a proof-of-concept demonstration to gain more concrete feedback.

A further possible stakeholder is the Federal Office of Civil Protection and Disaster Assistance, i.e. Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK) [47], under the Ministry of Interior. SUCCESS has not managed to organize an extensive exchange with BBK within the duration of the project, but it is planed that to be included as a potential stakeholder in the exploitation plans regarding the CI-SAN.

3.9 Irish Authorities

Likewise, SUCCESS has approached the Cyber-security centre in Ireland [48] and the Irish Defence Forces [49], as authorities that can foster the implementation of the SUCCESS architecture in Ireland, as well as EirGrid [50], the country's TSO.

The representative from the National Cyber Security centre in Ireland was very interested in the concepts that are developed within SUCCESS. He mentioned that there are a number of pan-European working groups that are working to develop mechanisms to deal with the cross-jurisdiction communication that is required to ensure effective management of cyber threats and incidents. The work being developed witihin SUCCESS to deal with this point should be well received by the authorities looking at this area. The NCSC stated that the work carried out in SUCCESS aligns with the National Institute of Standards and Technology (NIST) Directive well.

Contact was made to the Irish Defence Forces and the project and its concepts received positive response. A face to face meeting was not possible, but they will be in attendance at the final event in Dublin.

EirGird, the TSO in Ireland, were very receptive to the project. They stated that the work carried out in SUCCESS, unlike some other research projects, appeared to bring together many topics an themes in a constructive manner, where in other research projects each individual topic or issue is dealt with separately. Again, EirGrid expressed their opinion that the solutions being developed aligned very well with the NIST directive, and they welcomed the introduction of a structured manner for communication both between utilities within the same country, and also across international boundaries.

3.10 NATO

SUCCESS has further identified the North Atlantic Treaty Organization (NATO) [51] as a potential stakeholder in terms of critical infrastructure protection in times of escalated attacks beyond the civil – and terrorist related – context. Unfortunately, due to lack of relevant existing contacts, SUCCESS was unable to identify and exchange or disseminate substantial project content.

3.11 ENISA

The European Union Agency for Network and Information Security (ENISA) is an EU agency establishing supervisory and adisory connections with EU member states and private corporations in the area of cybersecurity. Among others, ENISA actively supports the pan-European Cyber Security Exercises, the development of National Cyber Security Strategies and performs studies related to the cyber security landscape in vertical sectors, the emergence of privacy preserving and ehancing technologies etc. The threat analysis conducted in SUCCESS was largely based on the ENISA threat taxonomy. SUCCESS actively monitored the activities of the agency, also inviting its members to the project meeting held in 12/13 June 2018 in Athens, in particular with the attendance of Dr. Konstantinos Moulinos and Dr. Christina Skouloudi to this meeting. Furthermore, contacts with ENISA, more specifically with Dr. Apostolos Malatras, have addressed the cyber security certification aspect. The related mandate for ENISA is expected later in 2018, so the respective SUCCESS deliverable D6.8 [4] will be disseminated as a potential input.

4. Potential future work

This deliverable presented the work of SUCCESS in different relevant standardization bodies and organizations as well towards policy makers. This work is part of the mid-term impact plan of SUCCESS. By nature, thus, the relevant work does not end with the end of the project itself. Most of the related work is part of the mid-to-long-term exploitation strategy of the SUCCESS partners and will be considered in the future.

We pinpoint the following examples that will continue beyond the end of the project in November 2018.

The work item at the ETSI TC Cyber has a planed schedule for publication in April 2019. The planed work includes the participation at the meetings, as well as the work on developing the included content beyond the current status, so as to reach an optimal maturity within the available time.

Furthermore, SUCCESS partners plan the continuation of initiated discussions with policy making entities and potential stakeholder organizations regarding the CI-SAN, towards achieving a higher impact and an estimation of the potential for developing the system to a higher TRL.

5. Conclusion

Over its duration of 30 months, SUCCESS has managed to disseminate content in form of presentations and discussions with the experts to a substantial number of standardization organizations. Moreover, SUCCESS has managed to include specific results in the ongoing work of standardization processes, most notably including one dedicated work item. Furthermore, SUCCESS heeding feedback towards the potential extended circle of stakeholders for the SUCCESS Security Solution and more specifically regarding the critical infrastructure security analytics network with a pan-European reach, has identified and addressed current relevant organizations, institutions and associations, both on national and international level.

This work is a significant part of the mid-term strategy for sustainable impact of the project, so that concrete technical and conceptual suggestions to real problems reach the market in the mid-term future. SUCCESS evaluates this work as a promising fruitful development with regards to the significant effect of the SUCCESS results towards enabling a secure smart grid, from the smart meter and a guarded smart metering process for both client and operator, over to a stable and resilient European energy grid.

6. References

[1] NobelGrid, "Nobel Grid project website," [Online]. Available: http://nobelgrid.eu/. [Accessed 30 September 2016].

[2] M. Simonov and G. Zanetto, "Agent-based protection of event-based smart meters," in *IEEE PES Innovative Smart Grid Technologies Conference Europe (ISGT-Europe)*, Torino, 2017.

[3] M. Simonov and G. Zanetto, "Secured event-based smart meter," in *3rd International Conference on Event-Based Control, Communication and Signal Processing (EBCCSP)*, Funchal, 2017.

[4] SUCCESS, "Deliverable D6.8 : Report on Certification Preparation, V2," 2018.

[5] SUCCESS, “Deliverable D6.5 : Report on Standardisation and Policies, V2,” 2017.

[6] ETSI, "Terms of Reference (ToR) for Technical Committee (TC) Cyber Security (CYBER)," ETSI Portal, [Online]. Available: https://portal.etsi.org/TBSiteMap/CYBER/CyberToR.aspx. [Accessed 30 September 2016].

[7] ETSI, "CYBER: Smart meter security guidelines," 2018. [Online]. Available: https://portal.etsi.org/webapp/WorkProgram/Report_WorkItem.asp?wki_id=54788. [Accessed 17 October 2018].

[8] ETSI, "Terms of Reference (ToR) for Technical Committee Machine-to-Machine communications (M2M)," ETSI Portal, [Online]. Available: https://portal.etsi.org/m2m/m2m_tor.asp. [Accessed 30 September 2016].

[9] OneM2M, "OneM2M Terms of Reference," [Online]. Available: http://member.onem2m.org/WebSite/ARC/ARC_TOR.aspx. [Accessed 30 September 2016].

[10] ETSI, "ETSI MEC Role and Activities," ETSI portal, [Online]. Available: http://www.etsi.org/technologies-clusters/technologies/mobile-edge-computing. [Accessed 30 September 2016].

[11] 3GPP, “SA1 - Services,” [Online]. Available: http://www.3gpp.org/Specifications-groups/sa-plenary/51-sa1-services. [Accessed 27 October 2017].

[12] 3GPP, “SA2 - Architecture,” [Online]. Available: http://www.3gpp.org/Specifications-groups/sa-plenary/53-sa2-architecture. [Accessed 27 October 2017].

[13] 3GPP, “Control and User Plane Separation of EPC nodes (CUPS),” [Online]. Available: http://www.3gpp.org/news-events/3gpp-news/1882-cups. [Accessed 27 October 2017].

[14] 3GPP, "3GPP SA6 Terms of reference," [Online]. Available: http://www.3gpp.org/specifications-groups/sa-plenary/sa6-mission-critical-applications. [Accessed 30 September 2016].

[15] FINESCE, "FINESCE project website," [Online]. Available: http://finesce.eu/. [Accessed 30 September 2016].

[16] C.-C.-E. CG-SEG, "Homepage," [Online]. Available: https://www.cencenelec.eu/standards/Sectors/SustainableEnergy/SmartGrids/Pages/default.aspx. [Accessed October 2018].

[17] CIGRE, "What-is-CIGRE," [Online]. Available: http://www.cigre.org/What-is-CIGRE. [Accessed 30 September 2016].

[18] C. B5, "What-is-SC-B5 - CIGRE," [Online]. Available: http://b5.cigre.org/What-is-SC-B5. [Accessed 30 September 2016].

[19] C. B3, "What-is-SC-B3 - Scope - CIGRE," [Online]. Available: http://b3.cigre.org/What-is-SC-B3/Scope. [Accessed 30 September 2016].

[20] C. D2, "What-is-SC-D2 - CIGRE," [Online]. Available: http://d2.cigre.org/What-is-SC-D2. [Accessed 30 September 2016].

[21] M. Sethi, J. Arkko, A. Keranen and H. Back, "Practical Considerations and Implementation Experiences in Securing Smart Object Networks," May 2018. [Online]. Available: https://tools.ietf.org/html/rfc8387. [Accessed 17 October 2018].

[22] J. Mattsson and M. Sethi, "Using EAP-TLS with TLS 1.3 draft-ietf-emu-eap-tls13-00," 29 May 2018. [Online]. Available: https://tools.ietf.org/html/draft-ietf-emu-eap-tls13-00. [Accessed 17 October 2018].

[23] T. Aura and M. Sethi, "Nimble out-of-band authentication for EAP (EAP-NOOB) draft-aura-eap-noob-03," 2 July 2018. [Online]. Available: https://tools.ietf.org/html/draft-aura-eap-noob-03. [Accessed 17 October 2018].

[24] T. Aura, "Nimble out-of-band authentication for EAP (EAP-NOOB)," 2017. [Online]. Available: https://github.com/tuomaura/eap-noob. [Accessed 17 October 2018].

[25] J. Arkko, V. Lehtovirta, V. Torvinen and P. Eronen, "Improved Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA') draft-ietf-emu-rfc5448bis-01," 2 July 2018. [Online]. Available: https://tools.ietf.org/html/draft-ietf-emu-rfc5448bis-01. [Accessed 17 October 2018].

[26] J. Arkko, K. Norrman and V. Torvinen, "Perfect-Forward Secrecy for the Extensible Authentication Protocol Method for Authentication and Key Agreement (EAP-AKA' PFS) draft-arkko-eap-aka-pfs-02," 2 July 2018. [Online]. Available: https://tools.ietf.org/html/draft-arkko-eap-aka-pfs-02. [Accessed 17 October 2018].

[27] P. Thubert, B. Sarikaya and M. Sethi, "Address Protected Neighbor Discovery for Low-power and Lossy Networks draft-ietf-6lo-ap-nd-06," 23 February 2018. [Online]. Available: https://tools.ietf.org/html/draft-ietf-6lo-ap-nd-06. [Accessed 17 Ocotber 2018].

[28] O. García-Morchon, S. Kumar and M. Sethi, "State-of-the-Art and Challenges for the Internet of Things Security draft-irtf-t2trg-iot-seccons-15," 19 May 2018. [Online]. Available: https://tools.ietf.org/html/draft-irtf-t2trg-iot-seccons-15. [Accessed 17 Ocotber 2018].

[29] Internet Architecture Board (IAB), "Managing Radio Networks in an Encrypted World (MaRNEW) Workshop 2015," 2015. [Online]. Available: https://www.iab.org/activities/workshops/marnew/. [Accessed 17 Ocotber 2018].

[30] WELMEC, "WELMEC 1 - An Introduction - A Guide," WELMEC Secretariat, www.welmec.org, 2016.

[31] WELMEC, "Software Guide (Measuring Instruments 2014/32/EU) - Working Group 7, Section 7.2," WELMEC Secretariat, www.welmec.org, 2015.

[32] ESMIG, "ESMIG website," [Online]. Available: http://esmig.eu/. [Accessed 30 September 2016].

[33] M. A. M. Association, "METERS AND MORE," [Online]. Available: http://www.metersandmore.com. [Accessed Oktober 2017].

[34] OSGP, "Open Smart Grid Protocoll website," [Online]. Available: http://www.osgp.org/what-is-osgp/. [Accessed 30 September 2016].

[35] DLMS, "DLMS User Group website," [Online]. Available: https://dlms.com/organization/generalinformation/index.html. [Accessed 30 September 2016].

[36] ENCS, "ENCS Homepage," [Online]. Available: https://www.encs.eu/. [Accessed 30 September 2016].

[37] European Commission, "The European Commission´s Competence Centre on Modelling," 2017.

[38] SUCCESS, "A European Security Analytics Network for Critical Infrastructures," *Whitepaper,* no. V2, 2018.

[39] TSCNET, “TSCNET website,” [Online]. Available: https://www.tscnet.eu/. [Accessed 20 March 2018].

[40] EE-ISAC, "Homepage," [Online]. Available: http://www.ee-isac.eu/. [Accessed October 2018].

[41] DENSEK, "Homepage," [Online]. Available: http://www.densek.eu/. [Accessed October 2018].

[42] EDRi, “About EDRi,” [Online]. Available: https://edri.org/about/. [Accessed 20 March 2018].

[43] Med-TSO, “About Med-TSO,” [Online]. Available: http://www.med-tso.com/mission.aspx?f=.

[44] ENTSO-E, "Homepage," [Online]. Available: https://www.entsoe.eu/. [Accessed October 2018].

[45] BSI, “BSI website,” [Online]. Available: https://www.bsi.bund.de/DE/Home/home_node.html. [Accessed 20 March 2018].

[46] B. KdoCIR, "Homepage," [Online]. Available: http://cir.bundeswehr.de/. [Accessed October 2018].

[47] BBK, “BBK website,” [Online]. Available: https://www.bbk.bund.de/EN/Home/home_node.html. [Accessed 20 March 2018].

[48] Department of Communications, Climate Action & Environment, “National Cyber Security Centre,” [Online]. Available: https://www.dccae.gov.ie/en-ie/communications/topics/Internet-Policy/cyber-security/national-cyber-security-centre/Pages/National-Cyber-Security-Centre.aspx. [Accessed 20 March 2018].

[49] Defence Forces Ireland, “Defence Forces Ireland website,” [Online]. Available: http://www.military.ie/en/home/. [Accessed 21 March 2018].

[50] EirGrid, “EirGrid website,” [Online]. Available: http://www.eirgridgroup.com/. [Accessed 20 March 2018].

[51] NATO, "Homepage," [Online]. Available: https://www.nato.int/. [Accessed October 2018].

[52] CEN-CENELEC, "CEN-CENELEC joint groups," [Online]. Available: http://www.cencenelec.eu/aboutus/Cooperation/Pages/default.aspx. [Accessed 30 September 2016].

[53] CIGRE, “CALL FOR PAPERS - SEERC CONFERENCE 2018,” [Online]. Available: http://www.cigre.org/Events/Other-CIGRE-Events/CALL-FOR-PAPERS-SEERC-CONFERENCE-2018. [Accessed 10 October 2017].

[54] National Power Summit, “National Power Summit website,” [Online]. Available: https://www.powersummit.ie/. [Accessed 26 October 2017].

[55] SUCCESS, “Deliverable D6.7 : Report on Certification Preparation, V1,” 2017.

7. List of Tables

8. List of Abbreviations

3GPP	3rd Generation Partnership Project
ACE	Authentication and Authorization for Constrained Environments
AMI	Advanced Metering Infrastructure
AMM	Advanced Meter Management
AMR	Automatic Meter Reading
API	Application Programming Interface
BBK	Bundesamt für Bevölkerungsschutz und Katastrophenhilfe
BR-GW	Breakout Gateway
BSI	Bundesamt für Sicherheit in der Informationstechnik
CBA	Cost and Benefit Analysis
CEN	Comité Européen de Normalisation
CENELEC	Comité Européen de Normalisation Electrotechnique
CG-SEG	Coordination Group on Smart Energy Grids
CGA	Cryptographically Generated Address
CI	Critical Infrastructure
CIGRE	International Council on Large Electric Systems
CI-SAN	Critical Infrastructure Security Analytics Network
CI-SOC	Critical Infrastructure Security Operation Centre
CoAP	Constrained Application Protocol
CORE	Constrained RESTful Environments
COSEM	COmpanion Specification for Energy Metering
CUPS	Control and User Plane Separation of EPC nodes
DENSEK	Distributed Energy Security Knowledge
DG CNECT	Dictorate-General for Communications Networks, Content and Technology
DG ENER	Dictorate-General for Energy
DG Home	Dictorate-General for Migration and Home Affairs
DLMS	Device Language Message Specification
DSM	Demand-Side-Management
DSO	Distributed System Operator
DTLS	Datagram Transport Layer Security
DTR	Draft Technical Report
EAP	Extensible Authentication Protocol
EAP-AKA	EAP Authentication and Key Agreement
EAP-NOOB	EAP Nimble out-of-band authentication
EBCCSP	Event-Based Control, Communication and Signal Processing
EDA	Event Driven Architecture
EDRi	European Digital Rights
EE-ISAC	European Energy – Information Sharing & Analysis Centre
EFTA	European Free Trade Association

EMS	Energy Management Systems
EMU	EAP Methods Update
ENCS	European Network for Cyber Security
ENISA	European Union Agency for Network and Information Security
ENTSO-E	European Network of Transmission System Operators for Electricity
EOS	European Organisation for Security
EPC	Evolved Packet Core
EPI	Electricity Power Industry
ESMIG	European Smart Metering Industry Group
ESMM	European Security Monitoring Matrix
ETSI	European Telecommunications Standards Institute
EU	European Union
EUI-64	Extended Unique Identifier 64
FINESCE	Future Internet Smart Utility Services
GDPR	General Data Protection Regulation
IAB	Internet Architecture Board
ICT	Information and Communication Technology
IEC	International Electro-technical Commission
IEEE	Institute of Electrical and Electronics Engineers
IESG	Internet Engineering Steering Group
IETF	Internet Engineering Task Force
IoT	Internet of Things
IP	Internet Protocol
IRSG	Internet Research Steering Group
ISGT	Innovative Smart Grid Technologies
ISO	International Organization for Standardization
IT	Information Technology
JRC	Joint Research Centre
JSON	JavaScript Object Notation
KdoCIR	Kommando Cyber- und Informationsraum
LWIG	Light-Weight Implementation Guidance
LWM2M	Lightweight Machine to Machine
MaRNEW	Managing Radio Networks in an Encrypted World
M2M	Machine to Machine
MEC	Mobile Edge Computing
Med-TSO	Mediterranean Transmission System Operators
MIDAS	Modelling Inventory Database and Access Services
MQTT	Message Queuing Telemetry Transport
NAT	Network Address Translation
NATO	North Atlantic Treaty Organization

NCSC	National Cyber Security Centre
NFV	Network functions virtualization
NIST	National Institute of Standards and Technology
NORM	New-generation Open Real-time smart Meter
OAuth	Open Authorization
OMA	Open Mobile Alliance
OOB	Out of Band
OSCORE	Object Security for Constrained RESTful Environments
PES	Power and Energy Society
PMU	Phasor Measurement Unit
PU	Public
PUF	Physically Unclonable Function
RAN	Radio Access Network
RFC	Request for Comments
RSA	Rivest, Shamir y Adleman cryptosystem
SA	Service and System Aspects
SC	Study Committees
SCADA	Supervisory Control and Data Acquisition
SDN	Software-Defined Networking
SDO	Standard Developing Organizations
SenML	Sensor Markup Language
SOA	Service-Oriented Architecture
STF	Specialist Task Force
SUIT	Software Updates for IoT
T2TRG	Thing-to-Thing Research Group
TB	Technical Board
TC	Technical Committee
TCP	Transmission Control Protocol
TLS	Transport Layer Security
TRL	Technology Readiness Level
TSO	Transmission System Operator
USA	United States of America
USMC	Utility Security Monitoring Centre
WELMEC	Western European Legal Metrology Cooperation
WG	Working Group
WI	Work Item
WP	Work Package
QoS	Quality of Service
ZVEI	Zentralverband Elektrotechnik- und Elektronikindustrie e.V.