Cybersecurity Certification Requirements for Supply Chain Services

Pinelopi Kyranoudi[1,2], Eleni-Maria Kalogeraki[1,2], Alexandra Michota[2,3], Nineta Polemi[2,4]
[1]MAGGIOLI SPA, Via Del Caprino 8, Santarcangelo Di Romagna 47822, Italy
[2]Department of Informatics, University of Piraeus, Karaoli and Dimitriou Str. 80, 18534 Piraeus, Greece
[3]FOCAL POINT SPRL, Avenue D'iena 11, 1410 Waterloo, Belgium
[4]trustilio B.V. , Vijzelstraat 68, 1017HL Amsterdam, The Netherlands

Email: pkyranoudi@unipi.gr, elmaklg@unipi.gr, amichota@focalpoint-sprl.be, dpolemi@gmail.com

Abstract—**Supply Chain Services (SCS) are the backbone of any economy and their security is most important for the competitiveness, prosperity and resilience of the European Digital Single Market. Security certification of the SCS is the necessary mitigation measure towards the trustworthiness of the digital economies. This paper presents the building blocks and requirements for the certification of the SCS.**

Keywords—Supply Chain Service, Target of Evaluation, European Cybersecurity Certification, Security, Conformity Assessment, Assurance.

I. Introduction

All critical sectors (e.g. transport, energy, health, economy) base their business activities on Supply Chain Services (SCS). Delivering goods (e.g. vehicles, pharmaceuticals, energy sources) is a SCS used by several sectors. For example, the pandemia, led the world to realise how important was the secure, global distribution and delivery of the vaccines [1]. SCS can be viewed as a web of many business partners, complex, interrelated processes using a chain of physical and cyber assets. SCS are attractive targets to adversaries exploiting their physical and cyber threats.

The most common threats of the SCS are: theft, environmental damage, masquerading of identities, terrorism, physical damage, strikes, eavesdropping, interception of emissions or sensitive information, assets hijacking, traffic manipulation, data poisoning data manipulation, social engineering, malware, identity or data priveleges abuse, manipulation of information, or even geolocalisation signals spoofing or jamming, failures and malfunctions of the cyber SCS assets.

The exploitation of these threats can lead to the disruption of the SCS and a variety of impacts, such as cargo and goods stealing, sensitive and critical data theft, illegal trafficking, systems damage or destruction, environmental disaster, or even human injuries or death. Additional impacts for the SCS providers and the involved business partners may include economic paralysis, financial loss and costs, kidnapping, fraud and money stealing are also in this long list, and all of the above usually come along with a tarnished reputation, and /or loss of competitiveness [2].

Ensuring the secure provision of the SCS at national, European and even more importantly at international level is a great challenge where security certification of the SCS can become a main mitigation measure. The European project CYRENE [3] and the national project CYSMET [4] that the authors work on, addresses the SCS security challenges.

This paper outlines some of these projects' findings, mainly the necessary aspects (e.g. standards, legal, security) which serve as building blocks for the proposal of a cybersecurity certification SCS scheme and the development of a conformity assessment methodology.

The remainder of this paper is structured as follows: Section II presents some generic classifications of SCS and the SCS security challenges and security objectives that are relevant to the current work. In section III, the relevant regulation and standards for SCS certification and the related requirements are analysed. In section IV, the Common Criteria (CC) [5] conformance requirements are addressed and the SCS is presented as a Target of Evaluation (ToE). Under this scope, associated security and assurance requirements are identified and described. Finally, section V draws the conclusions of the current work and presents our future research directions.

II. Security Of SCS

A. SCS classifications

According to the ISO 28000-series standards [6], supply chain functions are performed by a network of business partners (e.g. vendors, manufacturers, service providers, transportation centres, distributors, wholesalers, authorities). A variety of SCS management frameworks, e.g. [7;8] and SCS classifications can be found in the literature adopting business perspectives, such as the SCS pyramid of [9], which classifies SCS practices into managerial processes, information systems/technologies (IS/IT) and operational processes. In [10], a SCS configuration is introduced based on uncertainty and taxonomizes SCS into four types (efficient, risk-hedging, responsive and agile). A mapping of SCS strategic management views and SCS characteristics is proposed in [11] to provide a conceptual clustering of different management perspectives. A valid framework that measures SCS practices based on SCS management constructs (SCS integration, information sharing, customer service management, customer relationship, supplier relationship and postponement) is presented in [12]. Nevertheless, for assessing the cyber security risks of the

SCS (especially of the critical SCS) more information regarding SCS is needed.

With respect to [13], the security assessment (that will lead to certification) of the SCS requires their decomposition to its generic component: business processes, business partners and SCS assets (physical, cyber and people) involved in the provision of the SCS. To address this requirement, we developed a conceptual representation of the SCS approaching them under three different views: the overall business, the holistic technical and the sector-specific technical view of the SCS:

1) The SCS *overall business view* relies on the identification, analysis and assessment of any business driven SCS element that has a direct input for the provision of the SCS. As such, in this view, details of processes, business partners (i.e. suppliers, stakeholders, importers, vendors, manufacturers, authorities, governmental bodies) and their third parties, facilities, related business logic (e.g. data and information flows, decision making), and any legal/regulatory restrictions are considered.

2) The SCS *holistic-technical view* is an asset-based interdependent view of the SCS. It builds upon the previous view, i.e. it embeds all business processes, business partners and all cyber and physical assets hosted by the different business partners for the provision of the SCS processes. SCS asset models revealing asset-interdependencies accompany the presentation of the SCS under this view.

3) The SCS *sector-specific technical view* is an individual view (snapshot) of the SCS, i.e. the view that an individual business partner adopts: It consists of that business partner' processes and assets in the SCS (it is a segment of the SCS).

B. Security Challenges

The ISO/IEC 27000:2018 international standard [14], specifies the information security enablers of the CIA triad (Confidentiality, Integrity and Availability), including also the ensurance of other properties, such as authenticity, accountability, non-repudiation, and reliability. The maintenance of these outlined security features is capable of providing sustainable SCS. Existing best practices and guidelines for SCS security, may focus on these directions, but, notwithstanding, they are mostly focused on traditional security or procurement frameworks and they lack concentrating on the SCS self-insight [15].

SCS are recognized by the EU as global [16] and are considered as key-enablers for economic growth; thus the SCS management capability [17] is directly linked with the level of efficiency and effectiveness. SCS business partners keep a variety of SCS processes, critical ICT services and functions outsource supported through third parties and highly interdependent dispersed nodes of heterogeneous cyber-physical infrastructures. This fact limits their ability to control the entire ecosystem of the SCS hindering them to focus on the SCS self-insight, thereby raising their exposure to risks and threat propagation [15;17] that can jeopardize the continuity of the entire SCS (e.g. a cyber attack on a level gauging system of an oil tanker could produce service disruption and damage of the system that could lead to explosion and spill gallons of oil in the ocean causing serious environmental harm). According to the proposed NIS Directive 2 [18], addressing cyber risks of business partners involved within the SCS is the focal point to avoid coordinated supply chain attacks that could hardly impact the overall SCS performance. In this paper, we adopt the view that the business partners are responsible and are held accountable for their third parties (interacting with the SCS).

As the threat landscape is enormously evolving, the Regulation (EU) 2019/881 of the European Parliament and of the Council [16] (Cybersecurity Act) will promote the cybersecurity certification for ICT products (software, hardware, proccesses, services) and it will scale up the response to cyberattacks, promoting cyber resilience and trust for consumers within the EU. The European Cybersecurity Certification Scheme (EUCC) [19] will serve as a template in order to propose security certification schemes for ICT products. The CYRENE EU H2020 ongoing research project [3] aims to develop and propose a tailored and risk-based security and privacy certification scheme for the SCS based on the EUCC.

In this paper, we analyse the various security certification requirements for the SCS that CYRENE takes into account.

C. Security Objectives

Information security objectives have been identified as the objectives of an organization or an ICT product (hardware, software, system, service, process) that are in line with its information security policy to produce specific results [14]. Within the SCS, a security objective is considered to be the security that is required to bring the fulfilment of the SCS in consensus with the adopted security policy by the business partners involved [13]. In terms of security certification, the security objective is addressed as the intention to tackle detected SCS threats and/or meet the security policy of the SCS as has been agreed by all business partners involved [20].

The ETSI-TVRA methodology [21] orients security objectives, both to assets and their environments. The Cybersecurity Act [16], which is presented in the next section, emphasizes that a European cybersecurity certification scheme shall contain evaluation criteria and methods capable of demonstrating the security objectives of article 51: data protection against unauthorized handling, destruction or alteration, ensure that authorized people access to an organization's system is limited to their access rights, systematically record and timestamp access, use or process on data, services or functions and have the tangible possibility to know the actor's identity, identify vulnerabilities and dependencies, provide Vulnerability Assessment on assets and repair or resolve all known vulnerabilities detected, ensure that ICT products are secure by design and up-to-date, restore availability of data, services and functions in a timely manner in light of a security incident. The CC Evaluation [5], illustrated in section III, is capable of meeting such objectives through a group of candidate classes of Security Functional Requirements (SFRs) and Security Assurance Requirements (SARs) further described in section IV.

According to [19], presented in the next section, a party of certified products or an applicant to certification is proficient to determine the security objectives upon which an ICT product will be evaluated. The security objectives for a SCS adopting:

- the business view is the ensurance of the confidentiality, integrity, authenticity and non-repudiation of the SCS processes and business partners;
- the holistic technical view, is the ensurance of confidentiality, integrity, authenticity and non-repudiation of the entire SCS processes, business partners and SCS assets (physical and cyber);
- sector-specific technical view is the ensurance of confidentiality, integrity, authenticity and non-repudiation of the SCS processes and assets that the specific business partner are involved in and host respectively.

III. Certification Requirements Of SCS

In this section policy, legal and standardisation requirements for the cybersecurity certification of the SCS are presented.

A. Policy and Legal Requirements

Regarding the policy requirements, the following have been identified:

- Cybersecurity Act (CSA): The Regulation (EU) 2019/881 of the European Parliament and of the Council [16] puts the basis for the creation of the EU certification framework for ICT products; (it provides a framework based on standards, namely ISO/IEC 15408 [20] (also known as Common Criteria-CC-) and ISO/IEC 18045 [22]. The EU cybersecurity certification is defined as a comprehensive set of rules, technical requirements, standards and procedures that are established at Union level and that apply to the certification or Conformity Assessment (CA) of specific ICT products [22]. Each certification scheme shall specify the categories of products and services covered; the cybersecurity requirements that need to be met such as standards or technical specifications, the type of evaluation that is planned to be done such as self assessment or third party; and the intended level of assurance that is going to be achieved. The certificates will be valid across all Member States.
- European Cybersecurity Certification (EUCC): The EUCC scheme [19] based upon Article 54 of the CSA presented in detail the key elements that EU certification schemes shall include; it aims to serve as a successor to the existing schemes operating under the SOG-IS MRA [23]. It is more of a horizontal scheme, reusable by sectorial domains. It has been updated to EUCC v1.1.1., which has added the comments received via public consultation and recommendations given by the European Cybersecurity Certification Group (ECCG) [24].

Using the EUCC any ICT product can serve as a Target of Evaluation (ToE) and can be the subject of a security evaluation in which it is assessed against security requirements (CA) [5;20]. CA of the ToE is defined as the procedure that is followed for evaluating whether specified requirements relating to the ToE have been fulfilled [5]. On this account, ToE should be clearly identified and security aspects should be concretely specified in a CA process [20].

ToE can be the ICT product (equipment, device, asset, process or service) as a whole or the elements of the ICT product. In case the evaluation of a ToE contains only part of an IT product, ToE should not be misrepresented as the entire IT product. The CC leaves the assessor flexible what to evaluate not necessarily tied to the boundaries of IT products” [5].

- Based on the EUCC scheme, the EU cybersecurity certification scheme for Cloud Services (EUCS), has been prepared [25]. The EU Supply Chain Service cybersecurity certification (EUSCS) scheme needs to be based on the EUCC, take into account all relevant schemes (e.g. IoT scheme) and be developed in a way to improve the Internal Market conditions, to enhance the level of security of a wide range of SCS of the supply chain capabilities they implement, including application, infrastructure, and platform capabilities.

Legal requirements have also been identified in order to prepare the certification schemes:

- General Data Protection Regulation (GDPR): This is the regulation on the protection of natural persons with regard to the processing of personal data and on the free movement of such data [26]. Six data protection principles plus accountability are introduced by the GDPR. Accountability is the principle that creates an obligation for data controllers to comply with other principles as well as to be able to demonstrate it. The above mentioned principles shall be covered when preparing the EUSCS.
- Network and Information Security (NIS) Directive: This is the first legislative act [27] that is dedicated to cybersecurity imposing the obligation to assess and mitigate cyber risks, the set up a Computer Security Incident Response Team (CSIRT) and a national NIS authority. Compliance with NIS in the case of SCS will translate that the infrastructures of all business partners and their third parties will be NIS compliant and the SCS providers have the obligation to report any incidents in the local CERT or national CSIRT.
- The proposal of NIS 2.0 [18] contains measures for improving cybersecurity infrastructure and particularly the resilience and incident response capabilities of public and private competent authorities. One of the key elements of the Commission's proposal was to address security of supply chains and supplier relationships by requiring individual companies to address cybersecurity risks in supply chains and supplier relationships. The EUSCS scheme is considered to be a measure for mitigating such risks.

B. Interplay of Relevant Standards and Frameworks

Over time, the International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC) have developed many standards that can help establish, inter alia, proper risk management, security and CA systems. These standards are used by the organizations in order to achieve compliance with the above mentioned regulations e.g. NIS. GDPR, Cybersecurity Act.

1) Risk Management standards and frameworks

ISO/IEC 27000-series, also known as Information Security Management System (ISMS) Family of Standards, is a set of International Standards that are used to help organizations develop and implement a framework in order to manage information security risks and controls of their information assets as well as to prepare themselves to assess it. Some commonly used standards of this ISO/IEC series, which complement each other, are 27000:2018, 27001:2013, 27002:2013, 27005:2018, 27006:2015, 27110:2021 [14]. Definitions of risk management generic terms are presented in ISO Guide 73:2009 [28].

ISO 31000-series, is a family of risk management standards. In particular, ISO 31000:2018 [29] sets principles and generic guidelines on managing organisations' risks. Moreover, IEC 31010:2019 [30] on risk management-risk assessment techniques, sets guidance for selecting and applying techniques to assess risk in a wide range of situations.

NIST SP 800-37 Rev.2 [31] analyses a Risk Management Framework for information systems and organizations in terms of a system life-cycle approach for security and privacy and gives guidelines for the application of the framework to information systems and organizations.

2) SCS Security standards

ISO 28000-series of standards, is a set of requirements that organizations need to address in order to establish a management system to assure the quality or security of the aspects involved in the supply chain industry. The most commonly used standards of this series are ISO 28000:2007, also known as Supply Chain Security Management System (SCSMS), which introduces the specifications, and ISO 28001:2007, which provides best practices for SCS security implementation, assessments and plans, as well as the requirements and guidance [6;13].

3) IT Security Evaluation standards

ISO/IEC 15408 (CC) establishes the concepts, principles and techniques for IT security evaluation. The standard consists of three parts: the ISO/IEC 15408-1:2009 that introduces the general concepts and model, the ISO/IEC 15408-2:2008 that includes the security functional components and the ISO/IEC 15408-3:2008 that describes the security assurance components [20].

ISO/IEC 18045:2008 is a companion standard of ISO/IEC 15408 and provides a methodology to help an IT security evaluator to conduct a CC evaluation by defining the minimum actions to be performed [22].

4) CA standards

ISO/IEC 17000-series (17000:2020, 17020:2012, 17021, 17024:2012, 17067:2013) [32], is an international set of standards that mainly provides from the general concepts and principles for CA to guidelines and good practice recommendations. It also defines the requirements of bodies to be competent in performing reviews and inspection activities, as well as the ones they need to follow in order to approve a certification.

C. Interplay of Security Certification and Security Management

A glossary [33] interrelating certification and security concepts is under development by the CYRENE EU H2020 ongoing research project. In [33], the "Security Management (SM)" term is expressed by the ISO 28000:2007 definition, which considers all the activities and practices of organizations to manage security risks, threats, and impacts that are coordinated in a systematic, and optimized manner [6]. In addition, the glossary, according to the ISO/IEC 17021-1:2015, defines "certification" of a management system (e.g. environmental or quality or information security management system) as a means to assure that the organization has implemented a system to manage all relevant aspects of its activities, products and services covering the organization's policy and requirements of the relevant international management system standard [34].

As a consequence, SM's role is to give guidelines on how to administer the security-related aspects of an organization, whilst Security Certification includes SM, and in addition sets the requirements under which the organization can assure its security condition.

IV. Conformity Requirements Of SCS

A valuable CA process of SCS should meet the requirements generated from the CC for Information Technology Security Evaluation international standard [20]. Such requirements are considered as SCS conformity requirements. The SCS is presented and identified as Target of Evaluation (ToE) to show how it can be subject to a CA process and the specific conformity requirements addressing the SCS are emphasised.

A. CC Conformance Requirements

According to the CC [5], the distinction between security objectives and security requirements is of great importance. An objective is the expression of what a security system should be able to do in very broad terms while a requirement is a more detailed specification of how an objective is achieved. More than one requirement could be fulfilled in order to meet one objective. In ETSI TVRA methodology [21], indicative examples are presented in order to better apprehend this distinction between these two similar terms.

The security requirements consist of the following two categories:

- *Security Functional Requirements* (SFRs): SFRs is a set of requirements specified in the base security standard and an indication of where in the standard the detailed requirement can be found. In CC, SFRs are defined as a translation of the security objectives for the Target of Evaluation (ToE) into a standardised language. The implementation of functional requirements addresses the threats of counterfeited or tainted products and components.

- *Security Assurance Requirements* (SARs): Based on the CC, SARs provide a description of how assurance is to be gained that the ToE meets the SFRs. Evaluation Assurance Level (EAL) is a scale for measuring assurance for component ToE. In ETSI TVRA methodology, asset SARs provide an indication of the EAL that an implementation of the base security standard could be expected to meet.

From the Evaluation service level summary as specified in CC [5], Vulnerability analysis is the assurance class that will be used in CYRENE and it is adopted in this paper as well. This assessment deals with threats and could test if attackers are able to violate the SFRs. In particular, the vulnerability assessment class addresses the possibility of exploitable vulnerabilities introduced in the development or the operation of the ToE. Assessment of development vulnerabilities is covered by the assurance family AVA_VAN.

Cases where the security problem description mentions threats where the threat agent is very capable, and a low (or no) vulnerability analysis (AVA_VAN) are included in the SARs.

The security requirements of the SCS include:

- *Security by design*. The SCS provider and their business partners shall design and pre-configure the SCS processes and assets such that functionalities are based on well-established security practices
- *Least privilege*. The SCS provider and business partners shall design and pre-configure the processes and assets involved, according to the least privilege principle, whereby administrative rights are only used *when absolutely* necessary, sessions are technically separated and all accounts will be securely manageable;
- *Strong authentication*. The SCS provider and business partners shall provide and support strong authentication mechanisms for all accounts. If authentication is unsuccessful, the SCS processes will be interrupted or terminated (shall not allow any user specific activities to be performed);
- *Asset protection*. The SCS provider and business partners shall ensure that all processes and assets involved in the provision of the SCS are secure (confidentiality, integrity, authenticity, availability are met);
- *Supply Chain integrity*. The SCS provider and business partners should provide means to ensure that the SCS is genuine, cannot be tainted during operation, and its integrity is warranted throughout the SCS lifecycle;
- *Documentation transparency*. The SCS provider and business partners shall offer comprehensive and understandable documentation about the overall design of the SCS, describing its architecture, processes, business partners involved, assets, functionalities, implemented controls (and their documentations), individual SCS' security policies, the interfaces and interactions of components with each other and with internal and external services, in order to be able to implement and use the SCS in the most secure way possible. The SCS provider is obliged to manage an updated inventory with all reports (e.g. assessment/ audits/mutual agreements);
- *Quality management*. The SCS provider and business partners shall be able to provide evidence that a managed security by design approach has been adopted, including documented secure software development, quality management and information security management processes;
- *SCS business continuity*. The SCS provider and business partners shall guarantee support throughout the agreed lifetime of the SCS such that the SCS can work even after a successful attack, security breach or accident;
- *Conformance with law*. The SCS provider and business partners shall accept that all contracts (including those with subcontractors) are conform to the legal requirements in place and that the SCS operation is compliant with all security legislation, codes and guidelines (e.g. NIS I/II, Cybersecurity Act, GDPS, sector specific, e.g. IMO security guidelines, ISPS);
- *Information sharing*. All business partners and their third parties need to be obliged (via their Mutual Agreement) to share any information related to any incident, breach or attack of any element in the SCS;
- *Data usage restriction*. The SCS provider and business partners shall explicitly declare, justify and document, context and purpose wise, all data collection and processing activities that take or may take place, including relevant legal obligations stipulating them (e.g. GDPR).

B. SCS as Target of Evaluation

In this paper, the SCS is the Target of Evaluation (ToE); subjected to the CA process to evaluate whether the security requirements specified to a given SCS have been fulfilled. In addition, this work identifies the SCS-ToE in the scope of the three different conceptual views of the SCS, presented in section A: the overall business view (SCS-ToE I), the holistic technical view (SCS-ToE II) and the sector-specific technical view (SCS-ToE III) to give the opportunity to the SCS stakeholders to evaluate their SCS under any of these three different perspectives.

The SFRs and SARs of the SCS as ToE that constitute its objectives should be addressed for all SCS processes and assets.

C. SCS Security & Assurance Requirements

The SCS CA process is subject to the conformity definition, which embeds several abstract categories addressing the EU Commission New Legislative Framework (NLF) towards the single market for goods [35]. The NLF raises a package of measures to check the conformity of products (software, hardware, service) through several CA steps (e.g. testing, inspection, certification) to ensure that the products meet all legislative requirements before being placed in the market. Similarly, the SCS, which is considered as products that enfold a collection of procedures, partners and ICT assets, is required to follow such steps. Towards this concept, the CYRENE project, [3] in order to support the application and address the requirements of a proposed SCS certification scheme, it will develop and implement a novel dynamic cybersecurity and privacy CA process. The current research work initiates this idea by assessing the SCS security against its security and assurance requirements.

On this account, CA requirements are identified for the SCS-ToE addressing the corresponding assurance level “basic”, “substantial” or “high” that it may target [16] and the respective vulnerability analysis level of the assurance class of evaluation AVA: Vulnerability Assessment, that is adopted [5;19].

Moreover, the current work elicits the following CA requirements for the SCS-ToE in the scope of the three different conceptual SCS views, presented in section A. The SCS provider that seeks assessment, under a Mutual Recognition Agreement (MRA) of SCS business partners [19], delivers the SCS security certification schema (EUSCS-under development by the CYRENE H2020 project) to the assessor along with the specificities that have been followed to describe the SCS-ToE, i.e security-relevant sites explicitly required by a Protection Profile (PP), according to the adopted security certification schema.

- Define SCS-ToE’s sector environment (e.g. a vehicle transport SCS belongs in the automotive sectoral environment);
- Identify the perimeter of the assessment in terms of the assurance level and SCS view adopted;
- The assurance level of the SCS, will be considered “high”, if it is an essential service in the critical sectors of transport, energy, finance, health, government (as defined by NIS). Otherwise, the assurance level is Substantial (if the SCS belongs in a critical sector, but it is not essential) and Basic (for all other SCS).
- The degree of criticality of a SCS process will depend upon the impact(s) in relation to the provision of the SCS in case of its disruption/termination and the existence of appropriate business continuity measure(s). The criticality levels of the SCS assets will inherit the max degree of criticality of any of the processes that they participate.
- Conduct a SCS Mutual Recognition Agreement (MRA) between the involved SCS business partners to declare the conditions of recognition of the applied EUSCS, including the evaluation criteria and CA method relevant to the followed scheme, the desired level of assurance, their current security status, recognition of participants’ certificates, mitigation and individual security plans and responsibilities;
- In case the assurance level is “Basic”, self-assessment is feasible; otherwise the conformity assessment and the issuance of the certificate will be conducted by a certified Conformity Assessment Body (CAB) [19];
- The auditor checks all claims by the service provider and business partners and the security policies they adopt (from the MRA or PP) regarding the SCS-ToE;
- All security, individual documentations (e.g. security policies, incident response plans, contingency/ treatment/ business continuity plans) of the business partners are included in the signed SCS Mutual Recognition Agreement (MRA);
- The auditor depending on the adopted assurance level, evaluates whether privacy considerations and additional conventions described in the MRA and in SCS-ToE environment are fulfilled (e.g. for “basic” assurance level, the evaluation is based upon the business partners’ claims);
- The auditor conducts a CA process to evaluate whether the security requirements of the SCS-ToE, expressed in the PP, are fulfilled, according to the certification scheme;
- The CA process is driven by the requirements of the assurance level adopted (e.g. “high” assurance level is built on the efficiency testing of the resistance of the security functionalities).

V. Conclusions And Future Work

Supply Chain Services (SCS) are analysed from three different views in order to pave the way for their security certifications. In particular, we present the necessary relevant standards, legal frameworks and policies that reveal the certification requirements. Based on this analysis, the need for the provision of the SCS certification scheme (EUSCS) is evident. With this respect, the current work presents the SCS as a ToE for a CA process and based on the CC the security and assurance requirements for a SCS certification are identified. The analysis in this paper, provides the building blocks for a future development of the EUSCS. The identified cybersecurity requirements for SCS proposed in this paper can be considered by SCS organizations to orient their strategies accordingly to increase their preparedness, improve their cooperation with each other, adopt appropriate steps to manage security risks, report and handle security incidents with advancing ways, enable them to analyze relevant privacy concerns, promote trust and confidence to the European consumers and providers/suppliers and pave the way for a competitive and trustworthy Digital Single Market.

It is our intention to pursue this direction of research in the future, by developing and proposing a SCS certification scheme and a CA methodology, which will guide the assessors (CABs or self accessors) to implement the EUSCS independtly of the assurance level or complexity of the SCS. This future research work aims to enhance the security, privacy, resilience, accountability and trustworthiness of SCS.

Acknowledgment

This work has received funding from the European Union’s Horizon 2020 research and innovation action programme under grant agreement No 952690 project CYRENE.

In addition, it is supported by Partnership Agreement for the Development Framework 2014-2020, Operational program “Competitiveness, Entrepreneurship & Innovation” (EPAnEK), in the context of the project CYSMET: Integrated, Dynamic & Collaborative Risk Management System for Maritime Transport & Supply Chains, with project number: T2EΔK – 03488. The authors also thank all partners of these projects.

REFERENCES

[1] Maersk, “The challenges of the COVID-19 Vaccine global distribution: Analysis of the demanding logistics needs and sourcing expectations”. Online available: https://www.maersk.com/news/articles/2021/01/29/the-challenges-of-the-covid-19-vaccine-global-distribution, accessed on April 20 2021.

[2] ENISA, “Port Cybersecurity - Good practices for cybersecurity in the maritime sector”. Online available: https://www.enisa.europa.eu/publications/port-cybersecurity-good-practices-for-cybersecurity-in-the-maritime-sector, accessed on May 14 2021.

[3] CYRENE EU H2020 project. Online available: https://www.cyrene.eu, accessed on May 14 2021.

[4] CYSMET national project. Online available: https://cysmet.ubitech.eu, accessed on May 14 2021.

[5] Common Criteria for Information Technology Security Evaluation (CC) v3.1, Rev.5, 1/2/3: 201. Online available: https://www.commoncriteriaportal.org/cc/, accessed on April 29 2021.

[6] ISO 28000:2007 international standard, “Specification for security management systems for the supply chain”, 1st Edition 2007-09. Online available: https://www.iso.org/standard/44641.html, accessed on April 20 2021.

[7] D.M. Lambert,“Supply chain management: processes, partnerships and performance”, Supply Chain Management Institute, 2nd Edition, 2006.

[8] H. Kotzab., S. Seuring, M. Muller and G. Reiner (Eds), ”Research methodologies in supply chain management”; Physical-Verlag. A Springer Company, 2005.

[9] B. Ageron, O. Lavastre, and A. Spalanzani, "Innovative supply chain practices: the state of French companies", Supply Chain Management: An International Journal, Vol.18(3), 2013,pp.265 –276.

[10] H.L. Lee, “Aligning supply chain strategies with product uncertainties” California Management Review, Vol.44(3), pp. 105-119, 2002.

[11] G.A. Akyuz, and G. Gursoy, G. “Strategic management perspectives on supply chain”. Management Review Quarterly, 2019, pp. 1-29.

[12] A.B.L.E.S. Jabbour, A.B.N. Viana, and C.J.C. Jabbour, “Measuring supply chain management practices”, Measuring Business Excellence, 15(2), pp.18-31, 2011.

[13] ISO 28001:2007 international standard, “Security management systems for the supply chain - Best practices for implementing supply chain security, assessments and plans - Requirements and guidance”, 1st Edition 2007-09. Online available: https://www.iso.org/standard/45654.html, accessed on April 20 2021.

[14] ISO/IEC 27000-series on Information Security. Online available: https://www.iso.org/news/ref2266.html, accessed on April 29 2021.

[15] S. Papastergiou S., E.-M. Kalogeraki, D. Polemi, C. Douligeris, “Challenges and Issues in Risk Assessment of Modern Maritime Systems”, in Tsihrintzis G.A., Virvou M. (eds.), “Advances in Core Computer Science-Based Technologies. Papers in Honor of Professor Nikolaos Alexandris”, Springer, 2020, ISBN:978-3-030-41195-4.

[16] European Parliament and Council, Regulation (EU)2019/881 on ENISA and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act), April 2019.

[17] J. Boyens, C. Paulsen, N. Bartol, K. Winkler and J. Gimbi, “Key Practices in Cyber Supply Chain Risk Management: Observations from Industry” (NISTIR No 8276). National Institute of Standards and Technology, 2021.

[18] The Directive on security of network and information systems (NIS Directive 2). (2020, December 16). An official website of the European Union. Retrieved December 18, 2020, from https://ec.europa.eu/digital-single-market/en/directive-security-network-and-information-systems-nis-directive.

[19] ENISA, "Cybersecurity Certification EUCC, a candidate cybersecurity certification scheme to serve as a successor to the existing SOG-IS", v1.0, July 2020, Online available: https://www.enisa.europa.eu/publications/cybersecurity-certification-eucc-candidate-scheme, accessed on April 29 2021.

[20] ISO/IEC 15408-1/2/3:2008-09, international standard, “Information technology-Security techniques-Evaluation criteria for IT security”.

[21] ETSI TS 102 165-1, Cyber; Methods and protocols; Part 1: Method and pro forma for Threat, Vulnerability, Risk Analysis (TVRA), v5.2.3, 2017-10, Online available: https://www.etsi.org/deliver/etsi_ts/102100_102199/10216501/05.02.03_60/ts_10216501v050203p.pdf, accessed on April 29 2021.

[22] ISO/IEC 18045:2008 international standard, “Information technology-Security techniques- Methodology for IT security evaluation”, online available: https://www.iso.org/standard/46412.html, accessed on April 29 2021.

[23] SOG-IS, Online available: https://www.sogis.eu/, accessed on April 29 2021.

[24] ENISA, "Cybersecurity Certification EUCC, a candidate cybersecurity certification scheme to serve as a successor to the existing SOG-IS", v1.1.1, May 2021, Online available: https://www.enisa.europa.eu/publications/cybersecurity-certification-eucc-candidate-scheme-v1-1.1, accessed on May 27 2021.

[25] ENISA, "EUCS – Cloud Service Scheme: a candidate cybersecurity certification scheme for cloud services”. Online available: https://www.enisa.europa.eu/publications/eucs-cloud-service-scheme, accessed on April 29 2021.

[26] European Parliament and Council of the European Union. REGULATION (EU) 2016/679 (GDPR) Online available: EUR-Lex - 32016R0679 - EN - EUR-Lex (europa.eu)

[27] EU Council Directive on Network and Information Security (NIS Directive) 2016/1148/EU “concerning measures for a high common level of security of network and information systems across the Union”. Official Journal of the European Union L194 (19.7), 2016.

[28] ISO Guide 73:2009 "Risk management - Vocabulary" (2016). Online available: https://www.iso.org/standard/44651.html, accessed on April 29 2021.

[29] ISO 31000:2018 international standard, “Risk management-Guidelines”. Online available: https://www.iso.org/obp/ui/#iso:std:iso:31000:ed-2:v1:en, accessed on April 29 2021.

[30] IEC 31010:2019 international standard, "Risk management-Risk assessment techniques". Online available: https://www.iso.org/standard/72140.html, accessed on April 29 2021.

[31] NIST SP 800-37, Rev.2 , “Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy” (2018). Online available: https://csrc.nist.gov/publications/detail/sp/800-37/rev-2/final, accessed on April 29 2021.

[32] ISO/IEC 17000:2020 international standard, “Conformity assessment — Vocabulary and general principles”, 2nd Edition 2020-05. Online available: https://www.iso.org/standard/73029.html accessed on May 14 2021.

[33] CYRENE EU H2020 project, Glossary. Online available: https://www.cyrene.eu/glossary/ , accessed on April 29 2021.

[34] ISO/IEC 17021-1:2015 international standard, “Conformity assessment — Requirements for bodies providing audit and certification of management systems — Part 1: Requirements”, 1st Edition 2015-06. Online available: https://www.iso.org/standard/61651.html accessed on May 14 2021.

[35] European Commission, "Single Market for Goods", "New Legislative Framework". Online available: https://ec.europa.eu/growth/single-market/goods/new-legislative-framework_en, accessed on April 29 2021.