Horizon 2020 Program

ICT-02-2020

Building blocks for resilience in evolving ICT systems

Certifying the Security and Resilience of Supply Chain Services

D2.1: Supply Chain Analysis and Requirements

Contractual Date of Delivery	31/5/2021
Actual Date of Delivery	31/5/2021
Deliverable Security Class	Public
Type	Report
Editor	Jlenia Puma (CRF)
Contributors	Sofoklis Efremidis, Eleni-Maria Kalogeraki, Fabio De Donato, Cristiano Casadei (MAG) Jlenia Puma, Julien Mascolo (CRF) Danijela Boberic Krsticev (UNSPMF) Alexandra Michota, Nineta Polemi (FP) Nikos Argyropoulos (CLS) Manolis Chatzimpyrros (STS) Haralambos Mouratidis (SU) Gregory Chrysos (TSI) Farhan Sahito (PN)

	Pablo Giménez Salazar (VPF) Norma Zanetti (HYPER) Sophia Karagiorgou (UBI)
Quality Assurance	Nikos Argyropoulos (CLS)
Reviewers	George Spyridakis (ITML) Dora Kallipolitou (ZELUS)

Revision History

Version	Date	By	Overview
0.11	18/1/2021	All WP2 partners	Tentative ToC, unifying previous proposals
0.2	25/01/2021	CRF	Final ToC
0.2	26/02/2021	MAG, CRF, UNSPMF, FP, CLS, STS, SU, TSI, PN	First contributions provided
0.3	01/03/2021	CRF	Integration of contributions from the partners
0.3.1	09/03/2021	CRF	Minor modifications
0.3.1	19/03/2021	MAG, CRF, UNSPMF, FP, CLS, SU, VPF, HYPER	Update and integration to first contribution
0.4	25/03/2021	CRF	Integration of contributions from the partners
0.4.1	26/03/2021	CRF	Minor modifications
0.4.2	09/04/2021	MAG, CRF	Minor modifications
0.5	10/05/2021	CRF	Integration of contributions
0.5.1	13/05/2021	CRF, MAG, UBI, UNSPMF	Last contributions and modifications added before internal review
0.6	28/05/2021	CRF	Updated version incorporating input and comments from internal reviewers
1.0	31/05/2021	CRF	Final version

Table of Contents

List of Tables.....6

List of Figures.....8

List of Acronyms.....9

Executive Summary.....10

1. Introduction.....11

1.1 Scope.....11

1.2 Relation with other work packages and tasks.....12

1.3 Document Structure.....13

2. Security of Supply Chains.....**Error! Bookmark not defined.**

2.1 Supply Chain Classifications.....**Error! Bookmark not defined.**

2.1.1 Overall business view.....**Error! Bookmark not defined.**

2.1.2 Technical View - Asset Interdependent SC.....**Error! Bookmark not defined.**

2.1.3 Sector Specific view - SC snapshot.....**Error! Bookmark not defined.**

2.2 Security Aspects of the SCSs.....**Error! Bookmark not defined.**

2.2.1 SCS threat landscape.....**Error! Bookmark not defined.**

2.2.2 Legal framework.....**Error! Bookmark not defined.**

2.2.3 SC security standards (families of ISO2800x).....**Error! Bookmark not defined.**

2.2.4 Risk Management standards (families of ISO2700x) **Error! Bookmark not defined.**

2.2.5 SC risk assessment methodologies & Tools.....**Error! Bookmark not defined.**

3. EU Certification.....**Error! Bookmark not defined.**

3.1 Security Certification - EU requirements.....**Error! Bookmark not defined.**

3.1.1 Cybersecurity Act - The European certification legal instrument**Error! Bookmark not defined.**

3.1.2 Security Certification standards addressing EU requirements**Error! Bookmark not defined.**

3.1.3 The European Cyber Security Certification Schema (EUCC)**Error! Bookmark not defined.**

3.1.4 R&D certification projects and EU initiatives.....**Error! Bookmark not defined.**

3.1.5 Examples of Certificates.....**Error! Bookmark not defined.**

3.2 Conformity Assessment (CA).....**Error! Bookmark not defined.**

3.2.1 Basic Concepts and Requirements ..... **Error! Bookmark not defined.**

3.2.2 Target of Evaluations (ToE) - Security & Assurance Requirements**Error! Bookmark not defined.**

3.2.3 Methodologies for CAs..... **Error! Bookmark not defined.**

3.2.4 Standards for CAs ..... **Error! Bookmark not defined.**

3.2.5 Conformance monitoring..... **Error! Bookmark not defined.**

4. Methodology .....**Error! Bookmark not defined.**

4.1 Methodology for requirements elicitation.....**Error! Bookmark not defined.**

4.2 Methodology for requirements validation.....**Error! Bookmark not defined.**

4.3 CYRENE Questionnaire for enriching the requirements with feedback collected by external stakeholders .....**Error! Bookmark not defined.**

4.3.1 Feedback from the questionnaire..... **Error! Bookmark not defined.**

5. CYRENE Conformity Assessment.....**Error! Bookmark not defined.**

5.1 Targets of Evaluations (ToE) .....**Error! Bookmark not defined.**

5.1.1 ToE I: Business view of the VTS-SCS ..... **Error! Bookmark not defined.**

5.1.2 ToE II: Technical view of the VTS-SCS..... **Error! Bookmark not defined.**

5.1.3 ToE III: Sectorial view of the VTS-SCS ..... **Error! Bookmark not defined.**

5.2 Requirements for self-conformity assessing CYRENE ToEs**Error! Bookmark not defined.**

5.2.1 Requirements for CYRENE ToE I ..... **Error! Bookmark not defined.**

5.2.2 Requirements for CYRENE ToE II ..... **Error! Bookmark not defined.**

5.2.3 Requirements for CYRENE ToE III ..... **Error! Bookmark not defined.**

6. Conclusion .....**Error! Bookmark not defined.**

7. References .....**Error! Bookmark not defined.**

Appendix A – Glossary and Examples .....**Error! Bookmark not defined.**

Appendix B – Validation of CYRENE ToEs .....**Error! Bookmark not defined.**

B.1 CYRENE Advisory Boards .....**Error! Bookmark not defined.**

B.2 First Project Workshop .....**Error! Bookmark not defined.**

List of Tables

Table 1 - Impact on assets after a successful attack ..... **Error! Bookmark not defined.**
Table 2 - Mapping of motivation and capability of threat agents. . **Error! Bookmark not defined.**
Table 3 - Conformity standards. ..... **Error! Bookmark not defined.**
Table 4 - Business importance of SCS. ..... **Error! Bookmark not defined.**
Table 5 - Security standards and guidelines adopted. ..... **Error! Bookmark not defined.**
Table 6 - SC process description template. ..... **Error! Bookmark not defined.**
Table 7 - SCS Business Partners description template. ..... **Error! Bookmark not defined.**
Table 8 - ToE's infrastructure description template. ..... **Error! Bookmark not defined.**
Table 9 - "Vehicle Order Dispatch" process description. ..... **Error! Bookmark not defined.**
Table 10 - "Contract Agreement on the Vehicle Purchase" process description. .....**Error! Bookmark not defined.**
Table 11 - "Chartering Agreement Preparation and Negotiation" process description. .....**Error! Bookmark not defined.**
Table 12 - "Ship Formalities Arrangements" process description. **Error! Bookmark not defined.**
Table 13 - "Shipping Arrangements" process description. ..... **Error! Bookmark not defined.**
Table 14 - "Port Call Request" process description. ..... **Error! Bookmark not defined.**
Table 15 - "Standard Cargo Manifest" process description. ..... **Error! Bookmark not defined.**
*Table 16 - "Entry Summary Declaration (ENS)" process description.***Error! Bookmark not defined.**
Table 17 - "Loading and Discharge List" process description. ..... **Error! Bookmark not defined.**
Table 18 - "Discharge Vehicles" process description. ..... **Error! Bookmark not defined.**
Table 19 - "Customs Declarations" process description. ..... **Error! Bookmark not defined.**
Table 20 - "Transportation Order" process description. ..... **Error! Bookmark not defined.**
Table 21 - Business partners involved in the "Vehicles Order Dispatch" process. .....**Error! Bookmark not defined.**
Table 22 - Business partners involved in the "Contract Agreement on the Vehicle Purchase" process. ..... **Error! Bookmark not defined.**
Table 23 - Business partners involved in the "Chartering Agreement Preparation & Negotiation" process. ..... **Error! Bookmark not defined.**
Table 24 - Business partners involved in the "Ship Formalities Arrangements" processs. ...**Error! Bookmark not defined.**
Table 25 - Business partners involved in the "Shipping Arrangements" process. .....**Error! Bookmark not defined.**
*Table 26 - Business partners involved in the "Port Call Request" process.***Error! Bookmark not defined.**
Table 27 - Business partners involved in the "Standard Cargo Manifest" process. .....**Error! Bookmark not defined.**
*Table 28 - Business partners involved in the "Entry Summary Declaration (ENS)" process.***Error! Bookmark not defined.**
Table 29 - Business partners involved in the "Loading and Discharge List" process. .....**Error! Bookmark not defined.**
*Table 30 - Business partners involved in the "Discharge Vehicles" process.***Error! Bookmark not defined.**
*Table 31 - Business partners involved in the "Customs Declarations" process.***Error! Bookmark not defined.**

*Table 32 - Business partners involved in the “Transportation Order” process.***Error! Bookmark not defined.**
*Table 33 - Identified infrastructures of the “Port Call Request” process.***Error! Bookmark not defined.**
*Table 34 - Identified infrastructures of the “Standard Cargo Manifest” process.***Error! Bookmark not defined.**
Table 35 - Identified infrastructures of the “Entry Summary Declaration (ENS)” process.....**Error! Bookmark not defined.**
Table 36 - Identified infrastructures of the “Loading and Discharge List” process......**Error! Bookmark not defined.**
*Table 37 - Identified infrastructures of the “Discharge Vehicles” process.***Error! Bookmark not defined.**
*Table 38 - Identified infrastructures of the “Customs Declarations” processs.***Error! Bookmark not defined.**
*Table 39 - Identified infrastructures of the “Transportation Order” process.***Error! Bookmark not defined.**
*Table 40 - Supply of partial-assembled components process description.***Error! Bookmark not defined.**
Table 41 - “Supply of finished components” process description. **Error! Bookmark not defined.**
Table 42 - “Monitoring of components” process description. ..... **Error! Bookmark not defined.**
Table 43 - “Vehicle Assembly” process description. ..... **Error! Bookmark not defined.**
Table 44 - Business partners identification and analysis of the “Supply of partial-assembled components” process...... **Error! Bookmark not defined.**
Table 45 - Business partners identification and analysis of the “Supply of finished components” process. ..... **Error! Bookmark not defined.**
Table 46 - Business partners identification and analysis of the “Monitoring of components during transportation” process. ..... **Error! Bookmark not defined.**
Table 47 - Business partners identification and analysis of the “Vehicle Assembly” process. ..... **Error! Bookmark not defined.**
Table 48 - Identified infrastructures of the “Supply of partial-assembled components” process. ..... **Error! Bookmark not defined.**
Table 49 - Identified infrastructures of the "Supply of finished components" process. .....**Error! Bookmark not defined.**
Table 50 - Identified infrastructures of the "Monitoring of components" process......**Error! Bookmark not defined.**
*Table 51 - Identified infrastructures of the "Vehicle Assembly" process.***Error! Bookmark not defined.**
Table 52 - Requirements for CYRENE ToE I. ..... **Error! Bookmark not defined.**
Table 53 - Requirements for CYRENE ToE II...... **Error! Bookmark not defined.**
Table 54 - Requirements for CYRENE ToE III...... **Error! Bookmark not defined.**
*Table 55 - Extract from Security and Certification concept glossary.***Error! Bookmark not defined.**
*Table 56 - Extract from Supply Chain and Business concept glossary.***Error! Bookmark not defined.**
Table 57 - Extract from Maritime Transport concept glossary...... **Error! Bookmark not defined.**
Table 58 - Workshop agenda. ..... **Error! Bookmark not defined.**
Table 59 - Suggestions from the Advisory Boards...... **Error! Bookmark not defined.**

List of Figures

Figure 1 - Relation of WP2 with the other project WPs 13
Figure 2 - Ageron et al. Classification model ..... **Error! Bookmark not defined.**
Figure 3 - CYRENE circles of consideration for the CA process .. **Error! Bookmark not defined.**
Figure 4 - ISO28000 ..... **Error! Bookmark not defined.**
Figure 5 - Overview of requirements elicitation and validation process **Error! Bookmark not defined.**
Figure 6 - Overview of the methodology for requirements elicitation **Error! Bookmark not defined.**
Figure 7 - Cybersecurity activities frequency ..... **Error! Bookmark not defined.**
Figure 8 - Awareness of EU Cybersecurity Certification Framework for ICT products and services ..... **Error! Bookmark not defined.**
Figure 9 - Measures to address cybersecurity issues ..... **Error! Bookmark not defined.**
Figure 10 - Effective cybersecurity management plan applied to SCS **Error! Bookmark not defined.**
Figure 11 - Awareness of security standards and best practices adopted **Error! Bookmark not defined.**
Figure 12 - Security procedure - Number of respondents ..... **Error! Bookmark not defined.**
Figure 13 - Compliance with legal and regulatory principles and EU directives **Error! Bookmark not defined.**
Figure 14 - Experience of cybersecurity issues in last years ..... **Error! Bookmark not defined.**
Figure 15 - Probability of threats in the future ..... **Error! Bookmark not defined.**
Figure 16 - Addressee of risks and security threats ..... **Error! Bookmark not defined.**
Figure 17 - Relevant tools for secure service delivery ..... **Error! Bookmark not defined.**
Figure 18 - ICT Systems security measures applied to daily operations **Error! Bookmark not defined.**
Figure 19 - Perform of periodic audits ..... **Error! Bookmark not defined.**
Figure 20 - Analysis and evaluation of infrastructure security performed by external certified analyst ..... **Error! Bookmark not defined.**
Figure 21 - "Standard Cargo Manifest": a business process model example **Error! Bookmark not defined.**
Figure 22 - Business process model for the "Vehicle Order Dispatch" process **Error! Bookmark not defined.**
Figure 23 - Business process model for the "Contact Agreement on the Vehicle Purchase" process ..... **Error! Bookmark not defined.**
Figure 24 - Business process model for the "Chartering Agreement Preparation & Negotiation" process ..... **Error! Bookmark not defined.**
Figure 25 - Business process model for the "Ship Formalities Arrangements" process ..... **Error! Bookmark not defined.**
Figure 26 - Business process model for the "Shipping Arrangements" process **Error! Bookmark not defined.**
Figure 27 - Business process model for the "Port Call Request" process **Error! Bookmark not defined.**
Figure 28 - Business model for the "Standard Cargo Manifest" process **Error! Bookmark not defined.**

Figure 29 - Business process model for the “Entry Summary Declaration (ENS)” process..**Error! Bookmark not defined.**
Figure 30 - Business process model for the “Loading and Discharge List” process.....**Error! Bookmark not defined.**
*Figure 31 - Business process model for the “Discharge Vehicles” process***Error! Bookmark not defined.**
*Figure 32 - Business process model for the “Customs Declarations” process***Error! Bookmark not defined.**
*Figure 33 - Business process model for the “Transportation Order” process***Error! Bookmark not defined.**
Figure 34 - Business process model for the”Supply of partial-assembled components” process ..... **Error! Bookmark not defined.**
Figure 35 - Business process model for the "Supply of finished components" process .....**Error! Bookmark not defined.**
Figure 36 - Business process model for the "Monitoring of components" process.....**Error! Bookmark not defined.**
*Figure 37 - Business process model for the “Vehicle Assembly” process***Error! Bookmark not defined.**

List of Acronyms

Acronym	Description
AIS	Automatic identification system
BP	Business Partner
CA	Conformity Assessment
CC	Common Criteria
CII	Critical Information Infrastructure
CSA	Cybersecurity Act
ENS	Entry Summary Declaration
LNG	Liquefied Natural Gas
MRA	Mutual Recognition Agreement
PCS	Port Community System
PDCA	Plan-Do-Check-Act
RA	Risk Assessment
SC	Supply Chain
SCADA	Supervisory Control And Data Acquisition
SCRM	Supply Chain Risk Management
SCM	Standard Cargo Manifest
SCS	Supply Chain Service
SOG-IS	Senior Officials Group Information Systems Security
ToE	Target of Evaluation
TVRA	Threat Vulnerability Risk Analysis
VTS	Vehicle Transport Service

Executive Summary

The objective of this deliverable is to report the results of the activities performed in the first phase of CYRENE's Work Package 2. The main output is related to the requirements that have been collected from relevant standards and literature review, project pilot partners, as well as external stakeholders.

The document can be divided in four main parts. In the first one, an overview of the Supply Chains is given, describing both their classification, including three different views (business, technical and sectorial) of the SCs, and their security aspects, consisting of the threat landscape, legal framework, SC security and Risk Management standards and SC risk assessment methodology and tools.

In the second part, an overview of the EU Certification schemes is provided, encompassing the general definition and requirements (policy, legal, standards, methodologies, technical) regarding the security certification.

Moreover, in the third part, the document reports on the methodology used for collecting, analyzing and validating the requirements through the project's Advisory Boards. The feedback obtained from the proposed questionnaire for requirements validation are presented in this part and conclusions are drawn afterwards.

Finally, the fourth part of the deliverable deals with the three Targets of Evaluation (ToEs), namely, the Business, Technical, and Sectorial. Their descriptions and the respective validated requirements are provided in this section.

Two appendixes are included in the document. The first one gives information on a glossary that forms the basis of the concepts used in the project, while the second one gives details regarding the first workshop organized with the Advisory Boards at the end of the first six months of the project.

1. Introduction

1.1 Scope

This document is a record of the requirements that have been collected from several stakeholders, based on which the specifications of certification scheme, the definition of the conformity assessment processes, as well as the development and integration of tools within the CYRENE project will be developed.

The described outputs are the results of the activities performed during the following tasks:

- T2.1: Conformity and certification assessment scheme state of the art revision;
- T2.2: Large-scale European Supply Chain requirement gathering, analysis and tracking;
- T2.3: Legal and ethics requirements;
- T2.4: Classification of Supply Chains.

During the first task, the activities of CYRENE's phase 1 were initiated, focusing on the definition of a solid basis for setting up the CYRENE Conformity Assessment scheme. An updated state of the art analysis was carried out, consulting scientific papers, related projects, and relevant reference conformity assessment and certification schemes for cyber-security in related domains. In particular, during the task, the CYRENE consortium consulted and built upon the baseline security requirements recommended by ENISA **Error! Reference source not found.**. The existing relevant schemes are mapped to the four CYRENE circles of consideration (as described in **Error! Reference source not found.**), as well as to the three main aspects of CYRENE certification: business, infrastructure, and individual devices. Based on the described analysis, the task creates a basis for the conformity assessment scheme which grounds the multi-level evidence-driven supply chain risk assessment process.

During Task 2.2, in parallel to Task 2.1, the CYRENE consortium identified Supply Chains' Conformity Assessment requirements, along with legal/forensic, security and privacy requirements and covered the following aspects: (i) identification of requirements and specific needs of the participating Supply Chain Services, which represent different industry sub-sectors and with different needs with regard to IT security; (ii) substantial engagement of the participating SCs operators (representing different industrial sectors) so as to gain feedback regarding their needs and priorities in the frame of the project; (iii) specification of criteria associated to the nature of their IT system and infrastructure of SCs (such as size, interdependencies with other IT systems, services offered, etc.); (iv) analysis and documentation of the requirements of the various stakeholders, i.e. port authorities and operators, security systems integrators, policy makers etc.) in terms of the handling of multi-order dependencies and cascading effects; (v) identification and classification of dependencies between infrastructures and between SC operators, as well the dependencies among the business inter-organizational, infrastructure, and individual assets/devices.

The output of Task 2.3 is the identification, analysis and report of relevant legal and ethics requirements for CYRENE. The regulatory framework applicable to the project is analyzed to define requirements that are not dealt within the previous tasks.

Finally, Task 2.4 activities are focused on the specification of the criteria associated to the nature of IT systems and infrastructure of SCs (such as size, interdependencies with other IT systems,

services offered, number of administrators and IT security awareness level, etc.) based on which the categorization of the enterprise target group will occur.

1.2 Relation with other work packages and tasks

This document describes in detail the results of the Phase 1 activities of the project.

During Phase 2 of the project, whose main task is T2.5, the Conformity/Certification Assessment scheme set-up will be described. In fact, based on the results described in this document, the activities of this task will set up the proposed Conformity Assessment scheme for ensuring the security and resilience of Supply Chain Services. The proposed scheme will be the basis for the Conformity Assessment processes implemented in WP3 and WP4.

Moreover, Task 2.6 will propose a refined specification for CYRENE architecture based on a thorough understanding of the challenges, technologies, requirements and state-of-the-art introduced in all previous tasks of Work Package 2.

The result of this task will serve as a reference for the implementation phase of the CYRENE approach, defined in WP3 and WP4. In addition, it will serve as a reference and a starting point for the integration activities described in WP5. The interdependencies between WP2 and the rest of the Work Packages is depicted in *Figure 1*.

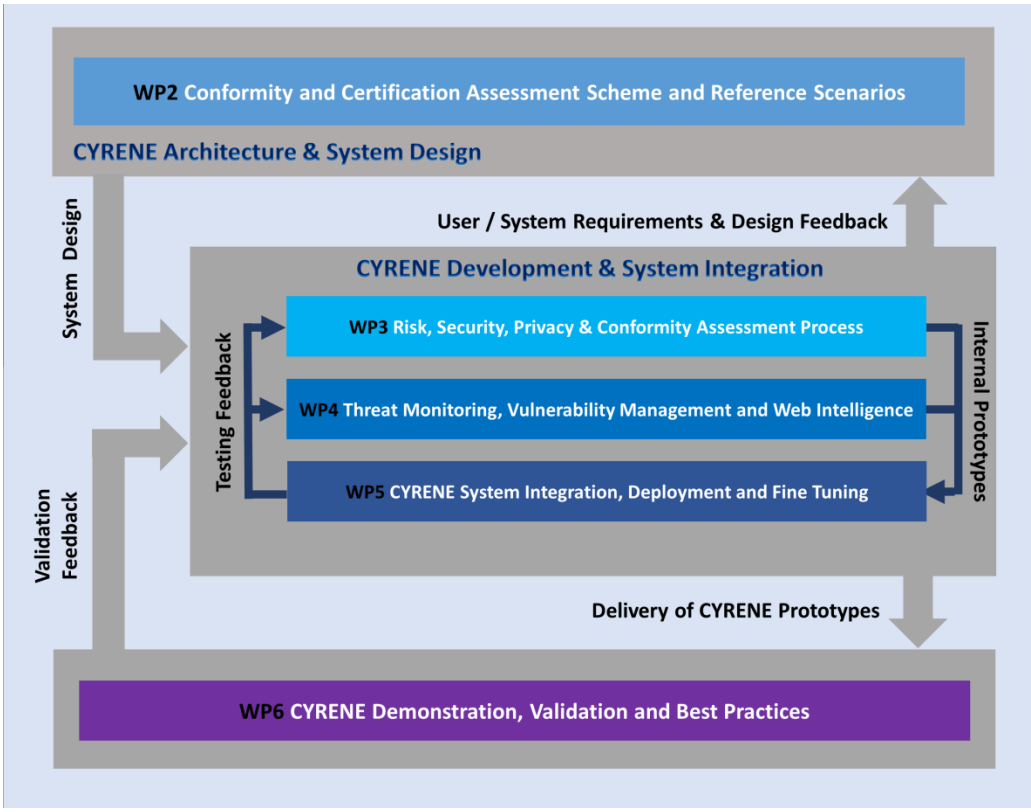

Figure 1 - Relation of WP2 with the other project WPs.

1.3 Document Structure

The rest of the document is structured as follows:

- Chapter 2 presents an overview of the Security of Supply Chains, describing how Supply Chains are classified and the security aspects of the involved Supply Chain Services.
- Chapter 3 gives an overview of the EU Certification schemes, presenting definitions and requirements that address the Security Certification process.
- Chapter 4 presents the Methodology used for requirements elicitation and their validation strategy.
- Chapter 5 presents the CYRENE Conformity Assessment process, including the description of the Targets of Evaluation and their requirements.
- Finally, Chapter 6 concludes the document.

DISCLAIMER: The document was submitted for revision to the EU Commission and is awaiting review and acceptance. Full access to its content will become available after this.