Horizon 2020 Program

ICT-02-2020

Building blocks for resilience in evolving ICT systems

Certifying the Security and Resilience of Supply Chain Services

D7.3: Mid-Term Standardization Activities Report

Contractual Date of Delivery	31/3/2022
Actual Date of Delivery	31/3/2022
Deliverable Security Class	Public
Type	Report
Editor	Farhan Sahito (PRI), Shivam Garg (PRI)
Contributors	Entire Consortium
Quality Assurance	Nikos Argyropoulos (CLS)
Reviewers	Nikos Argyropoulos (CLS), Gregory Chrysos (TSI)

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

Revision History

Version	Date	By	Overview
0.1	13/12/2021	PRIVANOVA	Basic draft with outline of the document
0.2	28/02/2022	PRIVANOVA	Revised draft
0.3	20/03/2022	All consortium partners	Revised draft with input for different sections from all consortium partners and feedback by reviewers
1.0	28/03/2022	PRIVANOVA	Final draft with all changes

Table of Contents

Index of Tables

List of Figures

List of Abbreviations

WP	Work Package
KPI	Key Performance Indication
ICT	Information & Communication Technologies
IoT	Internet of Things
IIoT	Industrial Internet of Things
CAP	Conformity Assessment Process
EU	European Union
DoW	Document of Work
EC	European Commission
R&I	Research & Innovation
SCADA	Supervisory control and data acquisition
4PL	Fourth Party Logistics
FCA	Free Carrier
Tbd	To be defined
GA	Grant Agreement
SCS	Supply Chain Systems
ISO	International Organization for Standardization
ETSI	European Telecommunications Standards Institute
ENISA	European Union Agency for Network and Information Security
IEEE	Institute of Electrical and Electronics Engineers
NIST	National Institute of Standards and Technology
CSIRT	Computer Security Incident Response Team
MS	Member State

Executive Summary

The EU funded project CYRENE aims at certifying the security and resilience of ICT supported supply chain services towards the objectives set forth by the European Cybersecurity Act. This deliverable serves as an initial report on the efforts and plans of the project consortium with regards to collaboration with the standardisation bodies and its contribution towards relevant existing standards. This deliverable also highlights various efforts, which have been made until now and the action plan going forward.

1. Introduction

This document will discuss the need and the relevance of CYRENE project with respect to industry standards and its interaction with them. The first section of this document introduces the deliverable purpose and its contents. The next sections highlight the background, current state of efforts as far as the input to standardization bodies and the planned future steps.

It is also noteworthy that all the partners make active effort to reach out to the standardization bodies, acquaint them with the objectives of the project and attempt to make the collaboration with such bodies smoother. We will also discuss the contribution by each partner in these activities under Section 3.2 of this document.

2. Background & context

2.1 Standardization needs

CYRENE project was envisaged to make key advances to the security, privacy, resilience, accountability, and trustworthiness of Supply Chains (SCs) through a novel and dynamic Conformity Assessment Process (CAP). This process evaluates the security services and the interconnected IT infrastructures and devices of the SCs. To ensure that the outcomes of this project are not limited to the lifetime of this project, it becomes necessary to contribute towards something more sustainable and widespread. Hence, the project consortium is making efforts to identify the primary outcomes, which can be connected to specific standardization bodies.

The CYRENE outcomes that are suitable for standardization are described below:1. The CYRENE glossary, which connects interrelated terms from the risk and conformity assessment, is suitable for ISO and ETSI.

2. The proposed CYRENE cybersecurity certification schema for the supply chain services will be a main outcome to communicate with ENISA for further consideration and standardization efforts.

3. The dual use of CYRENE risk/conformity assessment methodology is suitable for standardization efforts that deal with the implementation of certification standards (e.g., ETSI, ISO). An enhancement of the ETSI/TVRA methodology can be proposed to ETSI.

4. CYRENE proposed the development of an Information Security Management System (ISMS) for the SCS (Supply Chain Systems) based on ISO2800x and ISO2700x. This online SCS-ISMS will be operated by the SCS provider in collaboration with the business partners and it will support the SCS risk and conformity assessment processes. Particularly, SCS-ISMS can be a useful tool for the SCS provider and business partners to perform their risk assessment and update their -security policy and the Protection Profile (PP) with all security requirements. The SCS-ISMS can also be used by the accessor during the conformity assessment process to find the necessary evidence to assess the security requirements (claims in the SCS-PP) and evaluate the controls implemented if they meet the corresponding security requirements throughout specified period. The CYRENE ISMS can be of great interest to standardization bodies.

2.2 Current context of standardization in supply chains

Different standards are utilized depending on the assessment we need to conduct in a supply chain.

ISO 28000-series is a set of standards that are used for SCS risk assessment. This set of standards captures the requirements that organizations need to address to establish a management system to assure the quality or security of the aspects involved in the supply chain industry. In particular, the ISO 28000:2007 [1], also known as Supply Chain Security Management System (SCSMS), introduces the specifications, and the ISO 28001:2007 [2], provides the best practices for SCS security implementation, assessments, and plans, as well as the requirements and guidance.

When it comes to security controls, the ISO/IEC 27005 [3] and the ISO 28000 series provide a very good basis; however, these standards could not cover all the aspects that are related to the proposed EU cybersecurity certification scheme of SCS (EUSCS) [4]. Thus, the EUSCS also considered other families of standards such as NIST's SP 2000, which provide more focused controls for Federal supply chains extending the scheme application directives. The interplay and the compliance of these standards have been considered to simplify the evaluation process.

CYRENE proposed the development of an Information Security Management System (ISMS) for the SCS based on ISO2800x and ISO2700x [5].

[1] ISO - ISO 28000:2007 - Specification for security ...

[2] https://www.iso.org/standard/44641.html

[3] https://www.isms.online/iso-27005

[4] https://www.enisa.europa.eu/topics/standards/certification

[5] D. Polemi, A. Michota, S. Ioannidis, "A Proposed Cybersecurity Certification Scheme for Supply Chain Services", 5th NMIOTC (NATO Maritime Interdiction Operational Training Centre) Conference on Cyber Security in Maritime Domain, Souda Bay, Greece

3. Standardization Activities

This section lists and discusses various standardization bodies, which are relevant to this project and the main actions carried out until now with an intention of collaborating with them.

3.1 List of relevant standards

Standards play a key role in improving cyber defence and cybersecurity across different geographical regions and communities. Standardizing processes are essential to achieve effective cooperation in cross-border, cross-community, and cross-sector environments. The number of development organizations standards and published information security standards have increased in recent years, creating significant challenge. CYRENE has identified a set of standardization bodies and EU directives that must be closely monitored during the project lifetime, while specific contributions are envisaged to be provided. A feasibility study of a security labelling is one of the tasks pursued within CYRENE.

These bodies and announced strategies include:

- **The European Union Agency for Network and Information Security (ENISA):** ENISA [6] is a center of expertise for cybersecurity in Europe and supports MS for more than 10 years in implementing relevant EU legislation. ENISA sets up, develops, and enhances capabilities of CSIRTs across Europe and supports the development of cross-border communities committed to improve NIS throughput the EU. CYRENE aims to develop advanced technologies to achieve a higher maturity level of security incident detection and mitigation, which aligns with the ENISA goals. CYRENE is committed to establish a close collaboration with ENISA towards a common European privacy and cybersecurity standards framework. In addition, the consortium commits to share their results with ENISA and obtain knowledge through ENISA representatives.

- **The NIS Directive:** the EU directive [7] aims to create and strengthen a Computer Security Incident Response Team (CSIRT) Network to promote cooperation between all Member States (MS) and create a culture of security across sectors, such as digital infrastructure, manufacturing, transport, energy, healthcare, financial market and water. Given that the CYRENE framework targets SMEs/enterprises/orgnanisations in multiple sectors, adherence to this directive will be supported, while produced white papers on behalf of CYRENE consortium and information sharing can provide valuable information with regards to evolution of this directive. CYRENE can also contribute to good practices as well as risk analysis results, providing a common framework for information sharing across the EU.

- **The eIDAS Regulation (Regulation (EU) N°910/2014):** this regulation [8] creates among others a European internal market for electronic trust services – namely electronic signatures, electronic seals, time stamp, electronic delivery service and website authentication – by ensuring that they will work across borders and have the same legal status as traditional

[6] https://www.enisa.europa.eu/
[7] https://www.enisa.europa.eu/topics/nis-directive
[8] https://digital-strategy.ec.europa.eu/en/policies/eidas-regulation

paper-based processes. CYRENE aims at complying with eIDAS objectives and priorities.

- **The EU Cyber Security Strategy:** this strategy [9] provides a harmonized framework for the evolution of three different aspects of cybersecurity, which had been evolving independently until recently. Its central deliverable is the NIS Directive, which, in conjunction with the Directive 2013/40/EU, would require MS to have minimum NIS capabilities in place, and cooperate-exchange information within a dedicated network, and demand the private sector to adopt NIS enhancing actions. Towards this direction, the CYRENE complete cybersecurity platform can be disseminated appropriately and standardized to be widely used.

- **The Digital Agenda for Europe (DAE)**: The DAE [10] is Europe's strategy for a flourishing digital economy by 2020. Key action 6 of the DAE presents measures aiming at a reinforced and high-level NIS Policy and measures, allowing faster reactions in the event of cyber-attacks, including a Computer Emergency Response Team (CERT) for the EU institutions. CYRENE is in line with the main priorities set in the DAE for the forthcoming years (Trust & Security of this Agenda) and aims to disseminate its approach and outcomes to evolve the agenda.

- **The GSMA IoT Security Guidelines and Assessment:** GSMA [11] is a European standard organization that has delivered a set of IoT Security Guidelines, backed by an IoT Security Assessment scheme. The objective is to promote best practice for end-to-end security – from design to development and deployment of IoT services – and provide a mechanism to evaluate security measures. The CYRENE framework will adopt the guidelines offered by the GSMA and will disseminate its mechanisms to promote trustworthiness in supply chain for ICT systems/components in its entirety by addressing also the IoT ecosystems/devices that are part of the supply chain.

- **CEN-CENELEC-ETSI 'Cyber Security Coordination Group (CSCG)**: The group [12] intends to provide strategic advice in the field of IT security, Network and Information Security (NIS) and cybersecurity (CS). Contribution from CYRENE can be used towards the preparation of set of advice.

CYRENE aims at creating solid links and affect several cybersecurity, data protection and software standardisation initiatives significantly. More specifically, the following table lists indicative standards and regulations that will be considered:

[9] https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-strategy
[10] https://www.europarl.europa.eu/factsheets/en/sheet/64/digital-agenda-for-europe
[11] https://www.gsma.com/iot/iot-security/iot-security-guidelines/
[12] Coordination Group on Smart Energy Grids Cyber Security ...

Standards related to Information Security:

- ISO/IEC 27000 [13]: Information technology — Security techniques — Information security management systems — Overview and vocabulary
- ISO/IEC 27001:2013 [14] Information security management systems
- ISO/IEC 27002:2013 [15] Code of practice for information security controls
- ISO/IEC TR 20004:2015 [16] Information Technology-Security Techniques-Refining Software Vulnerability Analysis Under ISO/IEC 15408 And ISO/IEC 18045
- ISO/IEC 15408:2009 [17] Information Technology-Security Techniques-Evaluation criteria for IT security
- ISO/IEC 15443:2012 [18] Information Technology-Security Techniques-Security assurance framework
- ISO/IEC 15446:2017 [19] Information Technology-Security Techniques-Guidance to produce protection profiles and security target
- ISO/IEC 19790:2012 [20] Information Technology-Security Techniques-Security requirements for cryptographic modules
- ISO/IEC 19791:2010 [21] Information Technology-Security Techniques-Security assessment of operational systems
- ISO/IEC 19792:2009 [22] Information Technology-Security Techniques-Security evaluation of biometrics
- CSA Cloud Controls Matrix and PCI Data Security Standard [23]
- European Telecommunications Standards Institute (ETSI) [24] technical committee on information security indicators
- European Union Agency for Network and Information Security (ENISA) [25] and the communities issuing best practice and recommendation documents and guidelines on data protection

Standards related to Software Engineering:

- IEEE 12207-2017 [26] - ISO/IEC/IEEE International Standard - Systems and software engineering - Software life cycle processes
- ISO/IEC 15504 [27] Information technology – Process assessment, also termed Software Process Improvement and Capability Determination (SPICE)

[13] ISO - ISO/IEC 27000:2018 - Information technology ...
[14] ISO - ISO/IEC 27001 — Information security management
[15] ISO - ISO/IEC 27002:2013 - Information technology ...
[16] ISO - ISO/IEC TR 20004:2015 - Information technology ...
[17] ISO - ISO/IEC 15408-1:2009 - Information technology ...
[18] ISO - ISO/IEC TR 15443-1:2012 - Information technology ...
[19] ISO - ISO/IEC TR 15446:2017 - Information technology ...
[20] ISO - ISO/IEC 19790:2012 - Information technology ...
[21] ISO - ISO/IEC TR 19791:2010 - Information technology ...
[22] ISO - ISO/IEC 19792:2009 - Information technology ...
[23] Cloud Controls Matrix (CCM) - CSA
[24] ETSI - Welcome to the World of Standards!
[25] ENISA - Europa
[26] IEEE SA - IEEE/ISO/IEC 12207-2017
[27] ISO - ISO/IEC 15504-1:2004 - Information technology ...

Standards and Regulations related to Data protection and privacy: • General Data Protection Regulation GDPR 2016/679 [28] • ISO/IEC 29100:2011 [29] Privacy framework • CEN CWA 16113:2010 [30] Personal Data Protection Good Practices.
Standards related to Software development: • Software and systems engineering frameworks (ISO/IEC/IEEE 12207, 15288) [31] • Product quality (ISO/IEC 25000)[32] • Software testing (ISO/IEC 29119)[33] • Systems and software assurance (ISO/IEC 15026)[34]
Standards related to cybersecurity: • Technical communities of the Institute of Electrical and Electronics Engineers (IEEE) body on cloud computing and cybersecurity [35] • The International Organization for Standardization (ISO) [36] technical committee ISO/IEC JTC1 on information technology and specifically the working groups for the cloud computing fundamentals (SC38/WG3) and the SC7 committee on IT Security techniques • The cloud Security Alliance network, which deals with standardization on security practices and certification for cloud services, the National Institute of Standards and Technology (NIST) [37] working group on cloud computing security (NCC-SWG) • NIS
Standards related to Risk Management: ISO 31000 [38]Risk management – Guidelines

Table 1: Standards considered

[28] REGULATION (EU) 2016/ 679 OF THE EUROPEAN PARLIAMENT AND ...

[29] ISO - ISO/IEC 29100:2011 - Information technology ...

[30] BS CWA 16113 : PERSONAL DATA PROTECTION GOOD PRACTICES

[31] ISO/IEC 12207 and 15288 Systems and Software Engineering ...

[32] ISO - ISO/IEC 25000:2014 - Systems and software ...

[33] ISO - ISO/IEC/IEEE 29119-1:2013 - Software and systems ...

[34] ISO - ISO/IEC 15026-1:2013 - Systems and software ...

[35] IEEE SA - The IEEE Standards Association - Home

[36] ISO - International Organization for Standardization

[37] National Institute of Standards and Technology | NIST

[38] ISO - ISO 31000 — Risk management

3.2 Main actions carried out until now

The consortium has been actively discussing various possibilities and avenues to engage with the relevant standardization bodies. Other than identifying key organisations and relevant stakeholders, which we can reach out to, we have collated a list of all the interactions by consortium partners with all such bodies. Also, one of the key achievements until now is the preparation and dissemination of a whitepaper titled – “Contribution to Standardization” for relevant standardization bodies. This whitepaper is, also, uploaded to zenodo.org [39] for easier access and better dissemination. Lastly, this whitepaper is a result of collective input by all the consortium partners. Snapshots of this whitepaper are included in the Appendix.

Following is the list of contacts to which this whitepaper was shared by each partner:

Partner Name	Short Name	Dissemination Details
MAGGIOLI SPA	MAG	Whitepaper shared internally and to the EU funded project NESTOR
CENTRO RICERCHE FIAT SCPA	CRF	Whitepaper shared with partners in H2020 project related to cybersecurity CONCORDIA[40]
FUNDACION DE LA COMUNIDAD VALENCIANA PARA LA INVESTIGACION, PROMOCIONY ESTUDIOS COMERCIALES DE VALENCIAPORT	VPF	Whitepaper shared with port authority cyber-security department
STOCKHOLMS UNIVERSITET	SU	Whitepaper shared with research partners and with partners on INCIDENCE EU funded project.
TELECOMMUNICATION SYSTEMS INSTITUTE	TSI	Whitepaper shared with partners that work on IoT cybersecurity project: INTELLIOT[41]
University of Novi Sad Faculty of Sciences	UNSPMF	Whitepaper shared with partners in H2020-projects

[39] https://zenodo.org/record/6205417#.YisLeXpBy3A
[40] https://www.concordia-h2020.eu/
[41] https://intelliot.eu/

		related to cybersecurity: CII4IOT[42], COLLABS[43]
FOCAL POINT	FP	Whitepaper shared with ENISA standardisation team
PRIVANOVA SAS	PN	Whitepaper shared with members of ENISA, NIST and ISO
HYPERBOREA SRL	HYPER	Whitepaper shared with relevant stakeholders we cooperate with both in the academic and industrial sector.
CYBERLENS BV	CLS	Whitepaper disseminated both internally and with various partners CLS collaborates in different academic and industrial endeavours.
ZELUS IKE	ZELUS	Whitepaper shared with various partners of ZELUS and our collaborates
SPHYNX TECHNOLOGY SOLUTIONS AG	STS	Whitepaper shared with JCOP
IOTAM INTERNET OF THINGS APPLICATIONS AND MULTI LAYER DEVELOPMENT LTD	ITML	We shared with industrial partners that we deemed relevant. Additionally, we are part of the COLLABS and C4IIOT consortium (same as NOVISAD).
UBITECH LIMITED	UBI	Nothing to report

Table 2: Dissemination details of whitepaper

[42] https://www.c4iiot.eu/

[43] https://www.collabs-project.eu/

4. Future objectives and planned activities

4.1 Input from standardization bodies

PRIVANOVA got a response from members of ISO inviting CYRENE project to participate as a liaison for the relevant platform standards being developed. This was further passed on to consortium for evaluation to gauge feasibility and optimal action points on the project's end. PRIVANOVA had also shared a draft email to the partners to reach out to the relevant stakeholders.

Contributing to Standardization and certification activities, ZELUS reached out to its contacts cycle to disseminate the whitepaper of the CYRENE project with title "Contribution to Standardization - Certifying the Security and Resilience of Supply Chain Services". The goal of this activity and the scope of this whitepaper was to promote the outcomes of the CYRENE project, which are relevant to standardization bodies, and seek potential collaboration opportunities. As a result of the ZELUS' efforts, partners from the C4IIoT project [44] reached out inviting CYRENE for a presentation to its Spring School at the end of April 2022. Additionally, to this, a member of the MARVEL project [45] Greenroads Malta- showed their interest and introduced CYRENE representative to standardization expert enlisted by ENISA to the organization's pool of experts.

The whitepaper in general has been received highly by various relevant stakeholders related to standardization. We intend to keep this audience engaged with relevant content providing a basis for collaboration on standardization efforts.

4.2 Contribution to standardization bodies

Apart from the promotion and the contribution to the consortium efforts, i.e., the white paper mentioned earlier, ZELUS initiated a standardization activity as well. In more details, all ISO technical committees prepare a strategic business plan for their field of activity within 18 months of their creation. The strategic business plan describes the main aspects and the dynamics of the economic, social, regulatory, or other environment in which the committee operates, as well as its main objectives and current strategies, its internal structure, and the cooperation with other organizations. It includes the areas of activities of all the sub-committees operating under a technical committee. In that context, ISO invites members of the public and special interest groups to review any of these strategic business plans and to provide comments, which will be taken into consideration by the technical committee at its next review.

[44] https://www.c4iiot.eu/

[45] https://www.marvel-project.eu

ZELUS welcomed this invitation and has already made a preliminary search on the documents available for review as they are provided by the ISO technical committees. Within the following months, we are planning to coordinate a consortium initiative to provide collaboratively feedback to the committees for the following Strategic Business Plans:

- ISO/IEC JTC 1 that refers to Information technology Standards developed across domains.
- ISO/TC 176, which enlists standardization processes related to Quality Management & Quality Assurance across domains.
- ISO/TC 8 that is responsible for standardization related to the sector of ships and marine technology, and
- ISO/TC 272, which has been established to develop standards that relate to the delivery of forensic science services.

ZELUS is also working continuously on spotting relevant standards and related activities, as well as contributing to upcoming activities such as: the collaborative Application for ISO committee liaisons to contribute to the standardization work at ISO and more specifically to SC 27.

Other than this, PRIVANOVA maintains a live document to record, reach and exposure of each consortium partner with various relevant standardization bodies for boosting dissemination of standardization activities of the project

Overall, some of CYRENE partners co-operate in order to reach out to relevant stakeholders and work with them on standardization.

4.3 Fine-tuning collaboration opportunities

Going forward, the consortium will try to find opportunities (such as the one offered by ISO) to participate in relevant standardization bodies with specific capacity and role. Also, we intend to invite the right people from the standardization bodies to our project events and relevant meetings to increase the exposure of the project and its results. This two-pronged approach will ensure sustainable collaboration with such bodies.

5. Conclusions

CYRENE project is raising awareness about the project among standardization bodies and relevant associations proactively. The idea is to acquaint these bodies with the objectives and the results of this project and establish an active two-way communication channel. We have marked a start to this process with the help of the whitepaper discussed above. As we move forward, we will invite the relevant representatives from these standardization bodies in appropriate project meetings and events to make this collaboration stronger. All in all, as the project matures, the input to and from the standardization bodies is expected to increase considerably.

6. References

[1] ISO - ISO 28000:2007 - Specification for security ...

[2] https://www.iso.org/standard/44641.html

[3] https://www.isms.online/iso-27005

[4] https://www.enisa.europa.eu/topics/standards/certification

[5] D. Polemi, A. Michota, S. Ioannidis, “A Proposed Cybersecurity Certification Scheme for Supply Chain Services”, 5th NMIOTC (NATO Maritime Interdiction Operational Training Centre) Conference on Cyber Security in Maritime Domain, Souda Bay, Greece

[6] https://www.enisa.europa.eu/

[7] https://www.enisa.europa.eu/topics/nis-directive

[8] https://digital-strategy.ec.europa.eu/en/policies/eidas-regulation

[9] https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-strategy

[10] https://www.europarl.europa.eu/factsheets/en/sheet/64/digital-agenda-for-europe

[11] https://www.gsma.com/iot/iot-security/iot-security-guidelines/

[12] Coordination Group on Smart Energy Grids Cyber Security ...

[13] ISO - ISO/IEC 27000:2018 - Information technology ...

[14] ISO - ISO/IEC 27001 — Information security management

[15] ISO - ISO/IEC 27002:2013 - Information technology ...

[16] ISO - ISO/IEC TR 20004:2015 - Information technology ...

[17] ISO - ISO/IEC 15408-1:2009 - Information technology ...

[18] ISO - ISO/IEC TR 15443-1:2012 - Information technology ...

[19] ISO - ISO/IEC TR 15446:2017 - Information technology ...

[20] ISO - ISO/IEC 19790:2012 - Information technology ...

[21] ISO - ISO/IEC TR 19791:2010 - Information technology ...

[22] ISO - ISO/IEC 19792:2009 - Information technology ...

[23] Cloud Controls Matrix (CCM) - CSA

[24] ETSI - Welcome to the World of Standards!

[25] ENISA - Europa

[26] IEEE SA - IEEE/ISO/IEC 12207-2017

[27] ISO - ISO/IEC 15504-1:2004 - Information technology ...

[28] REGULATION (EU) 2016/ 679 OF THE EUROPEAN PARLIAMENT AND ...

[29] ISO - ISO/IEC 29100:2011 - Information technology ...

[30] BS CWA 16113 : PERSONAL DATA PROTECTION GOOD PRACTICES

[31] ISO/IEC 12207 and 15288 Systems and Software Engineering ...

[32] ISO - ISO/IEC 25000:2014 - Systems and software ...

[33] ISO - ISO/IEC/IEEE 29119-1:2013 - Software and systems ...

[34] ISO - ISO/IEC 15026-1:2013 - Systems and software ...

[35] IEEE SA - The IEEE Standards Association - Home

[36] ISO - International Organization for Standardization

[37] National Institute of Standards and Technology | NIST

[38] ISO - ISO 31000 — Risk management

[39] https://zenodo.org/record/6205417#.YisLeXpBy3A

[40] https://www.concordia-h2020.eu/

[41] https://intelliot.eu/

[42] https://www.c4iiot.eu/

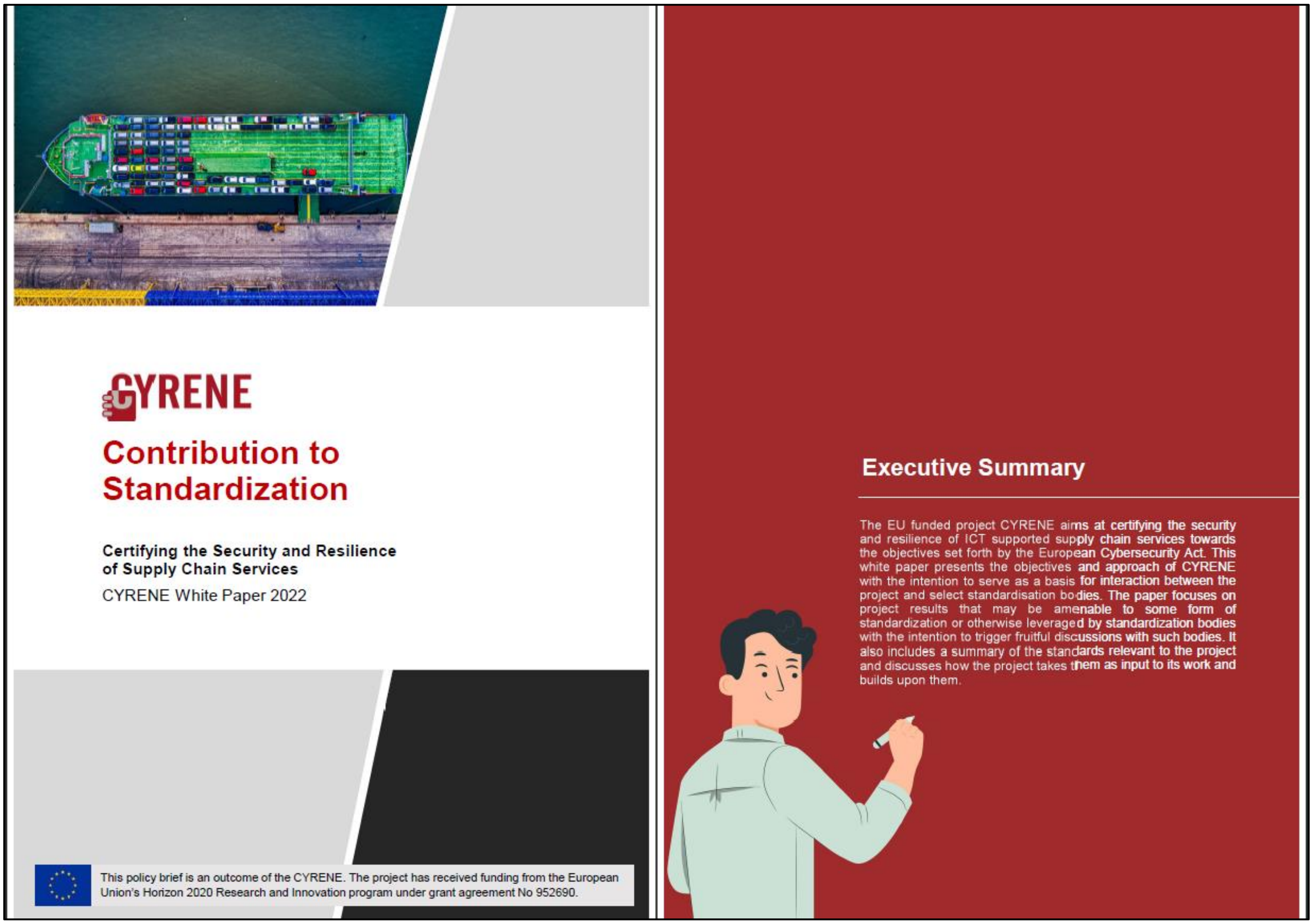
[43] https://www.collabs-project.eu/

[44] https://www.c4iiot.eu/

[45] https://www.marvel-project.eu

7. Appendix

Snapshots of the whitepaper



CYRENE

Contribution to Standardization

Certifying the Security and Resilience of Supply Chain Services

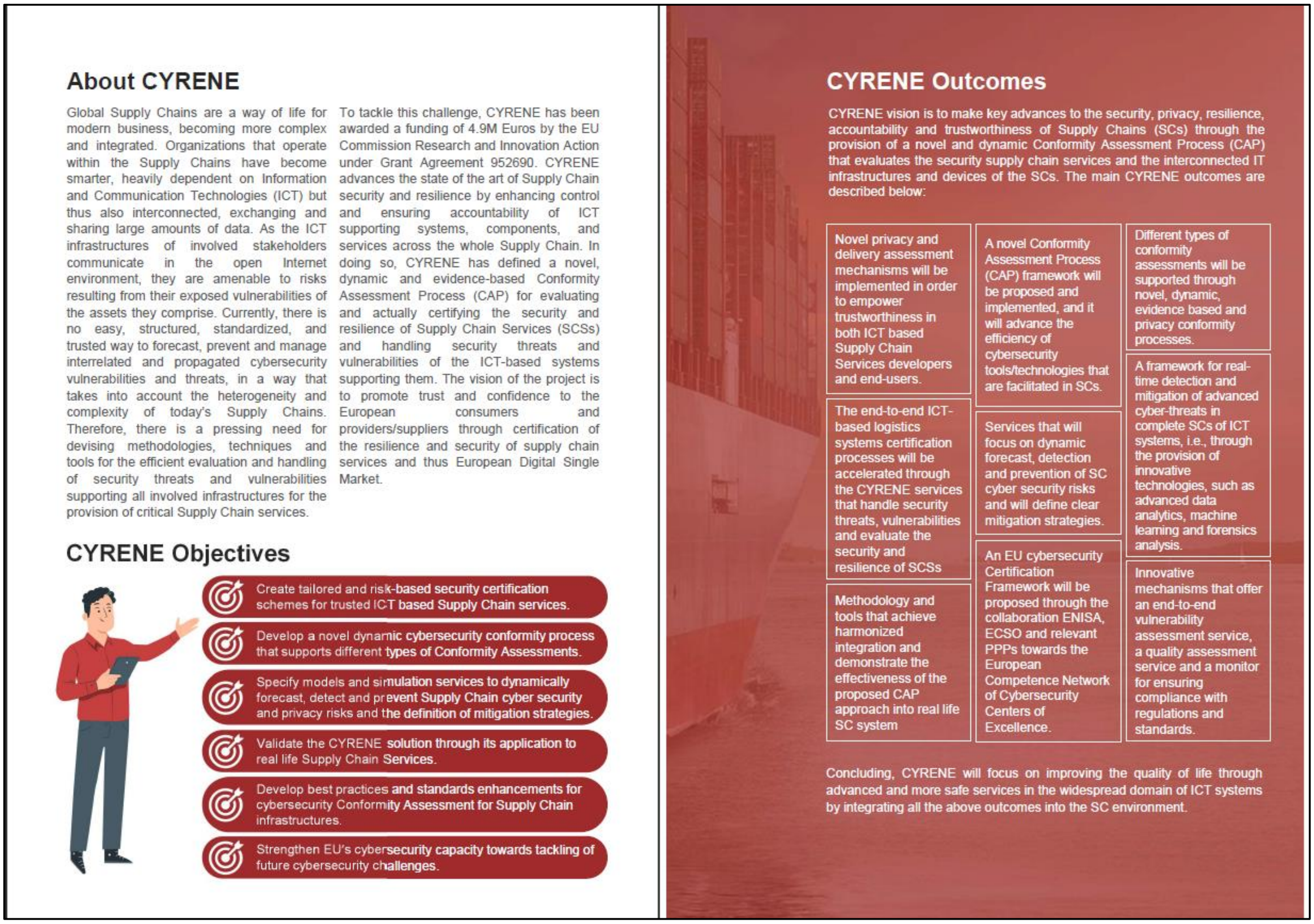
CYRENE White Paper 2022

This policy brief is an outcome of the CYRENE. The project has received funding from the European Union's Horizon 2020 Research and Innovation program under grant agreement No 952690.

Executive Summary

The EU funded project CYRENE aims at certifying the security and resilience of ICT supported supply chain services towards the objectives set forth by the European Cybersecurity Act. This white paper presents the objectives and approach of CYRENE with the intention to serve as a basis for interaction between the project and select standardisation bodies. The paper focuses on project results that may be amenable to some form of standardization or otherwise leveraged by standardization bodies with the intention to trigger fruitful discussions with such bodies. It also includes a summary of the standards relevant to the project and discusses how the project takes them as input to its work and builds upon them.

Figure 1: Whitepaper (Page 1 of 5)



About CYRENE

Global Supply Chains are a way of life for modern business, becoming more complex and integrated. Organizations that operate within the Supply Chains have become smarter, heavily dependent on Information and Communication Technologies (ICT) but thus also interconnected, exchanging and sharing large amounts of data. As the ICT infrastructures of involved stakeholders communicate in the open Internet environment, they are amenable to risks resulting from their exposed vulnerabilities of the assets they comprise. Currently, there is no easy, structured, standardized, and trusted way to forecast, prevent and manage interrelated and propagated cybersecurity vulnerabilities and threats, in a way that takes into account the heterogeneity and complexity of today's Supply Chains. Therefore, there is a pressing need for devising methodologies, techniques and tools for the efficient evaluation and handling of security threats and vulnerabilities supporting all involved infrastructures for the provision of critical Supply Chain services.

To tackle this challenge, CYRENE has been awarded a funding of 4.9M Euros by the EU Commission Research and Innovation Action under Grant Agreement 952690. CYRENE advances the state of the art of Supply Chain security and resilience by enhancing control and ensuring accountability of ICT supporting systems, components, and services across the whole Supply Chain. In doing so, CYRENE has defined a novel, dynamic and evidence-based Conformity Assessment Process (CAP) for evaluating and actually certifying the security and resilience of Supply Chain Services (SCSs) and handling security threats and vulnerabilities of the ICT-based systems supporting them. The vision of the project is to promote trust and confidence to the European consumers and providers/suppliers through certification of the resilience and security of supply chain services and thus European Digital Single Market.

CYRENE Objectives

- Create tailored and risk-based security certification schemes for trusted ICT based Supply Chain services.
- Develop a novel dynamic cybersecurity conformity process that supports different types of Conformity Assessments.
- Specify models and simulation services to dynamically forecast, detect and prevent Supply Chain cyber security and privacy risks and the definition of mitigation strategies.
- Validate the CYRENE solution through its application to real life Supply Chain Services.
- Develop best practices and standards enhancements for cybersecurity Conformity Assessment for Supply Chain infrastructures.
- Strengthen EU's cybersecurity capacity towards tackling of future cybersecurity challenges.

CYRENE Outcomes

CYRENE vision is to make key advances to the security, privacy, resilience, accountability and trustworthiness of Supply Chains (SCs) through the provision of a novel and dynamic Conformity Assessment Process (CAP) that evaluates the security supply chain services and the interconnected IT infrastructures and devices of the SCs. The main CYRENE outcomes are described below:

Novel privacy and delivery assessment mechanisms will be implemented in order to empower trustworthiness in both ICT based Supply Chain Services developers and end-users.

The end-to-end ICT-based logistics systems certification processes will be accelerated through the CYRENE services that handle security threats, vulnerabilities and evaluate the security and resilience of SCSs

Methodology and tools that achieve harmonized integration and demonstrate the effectiveness of the proposed CAP approach into real life SC system

A novel Conformity Assessment Process (CAP) framework will be proposed and implemented, and it will advance the efficiency of cybersecurity tools/technologies that are facilitated in SCs.

Services that will focus on dynamic forecast, detection and prevention of SC cyber security risks and will define clear mitigation strategies.

An EU cybersecurity Certification Framework will be proposed through the collaboration ENISA, ECSO and relevant PPPs towards the European Competence Network of Cybersecurity Centers of Excellence.

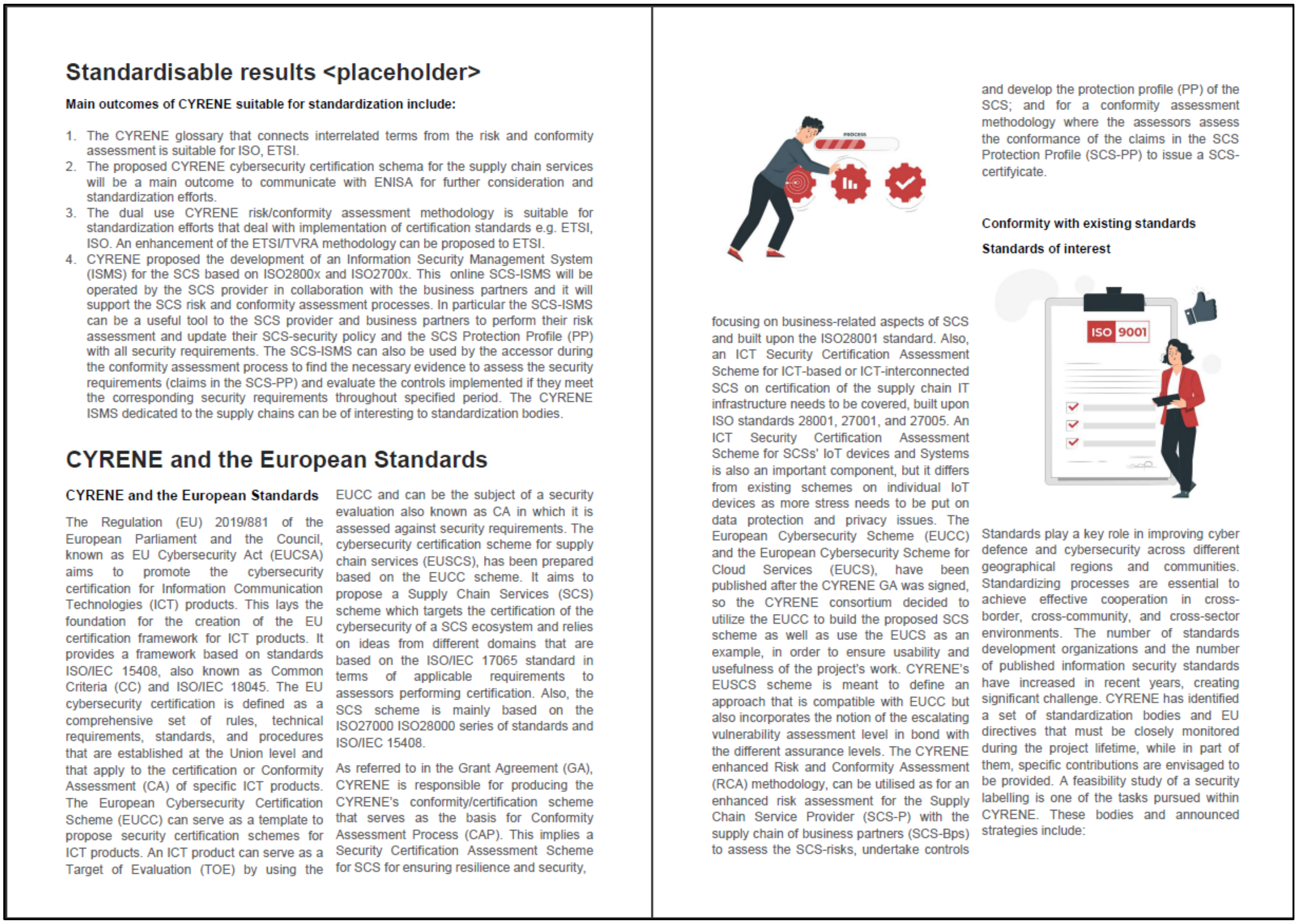
Different types of conformity assessments will be supported through novel, dynamic, evidence based and privacy conformity processes.

A framework for real-time detection and mitigation of advanced cyber-threats in complete SCs of ICT systems, i.e., through the provision of innovative technologies, such as advanced data analytics, machine learning and forensics analysis.

Innovative mechanisms that offer an end-to-end vulnerability assessment service, a quality assessment service and a monitor for ensuring compliance with regulations and standards.

Concluding, CYRENE will focus on improving the quality of life through advanced and more safe services in the widespread domain of ICT systems by integrating all the above outcomes into the SC environment.

Figure 2: Whitepaper (Page 2 of 5)



Standardisable results <placeholder>

Main outcomes of CYRENE suitable for standardization include:

1. The CYRENE glossary that connects interrelated terms from the risk and conformity assessment is suitable for ISO, ETSI.
2. The proposed CYRENE cybersecurity certification schema for the supply chain services will be a main outcome to communicate with ENISA for further consideration and standardization efforts.
3. The dual use CYRENE risk/conformity assessment methodology is suitable for standardization efforts that deal with implementation of certification standards e.g. ETSI, ISO. An enhancement of the ETSI/TVRA methodology can be proposed to ETSI.
4. CYRENE proposed the development of an Information Security Management System (ISMS) for the SCS based on ISO2800x and ISO2700x. This online SCS-ISMS will be operated by the SCS provider in collaboration with the business partners and it will support the SCS risk and conformity assessment processes. In particular the SCS-ISMS can be a useful tool to the SCS provider and business partners to perform their risk assessment and update their SCS-security policy and the SCS Protection Profile (PP) with all security requirements. The SCS-ISMS can also be used by the accessor during the conformity assessment process to find the necessary evidence to assess the security requirements (claims in the SCS-PP) and evaluate the controls implemented if they meet the corresponding security requirements throughout specified period. The CYRENE ISMS dedicated to the supply chains can be of interesting to standardization bodies.

CYRENE and the European Standards

CYRENE and the European Standards

The Regulation (EU) 2019/881 of the European Parliament and the Council, known as EU Cybersecurity Act (EUCSA) aims to promote the cybersecurity certification for Information Communication Technologies (ICT) products. This lays the foundation for the creation of the EU certification framework for ICT products. It provides a framework based on standards ISO/IEC 15408, also known as Common Criteria (CC) and ISO/IEC 18045. The EU cybersecurity certification is defined as a comprehensive set of rules, technical requirements, standards, and procedures that are established at the Union level and that apply to the certification or Conformity Assessment (CA) of specific ICT products. The European Cybersecurity Certification Scheme (EUCC) can serve as a template to propose security certification schemes for ICT products. An ICT product can serve as a Target of Evaluation (TOE) by using the EUCC and can be the subject of a security evaluation also known as CA in which it is assessed against security requirements. The cybersecurity certification scheme for supply chain services (EUSCS), has been prepared based on the EUCC scheme. It aims to propose a Supply Chain Services (SCS) scheme which targets the certification of the cybersecurity of a SCS ecosystem and relies on ideas from different domains that are based on the ISO/IEC 17065 standard in terms of applicable requirements to assessors performing certification. Also, the SCS scheme is mainly based on the ISO27000 ISO28000 series of standards and ISO/IEC 15408.

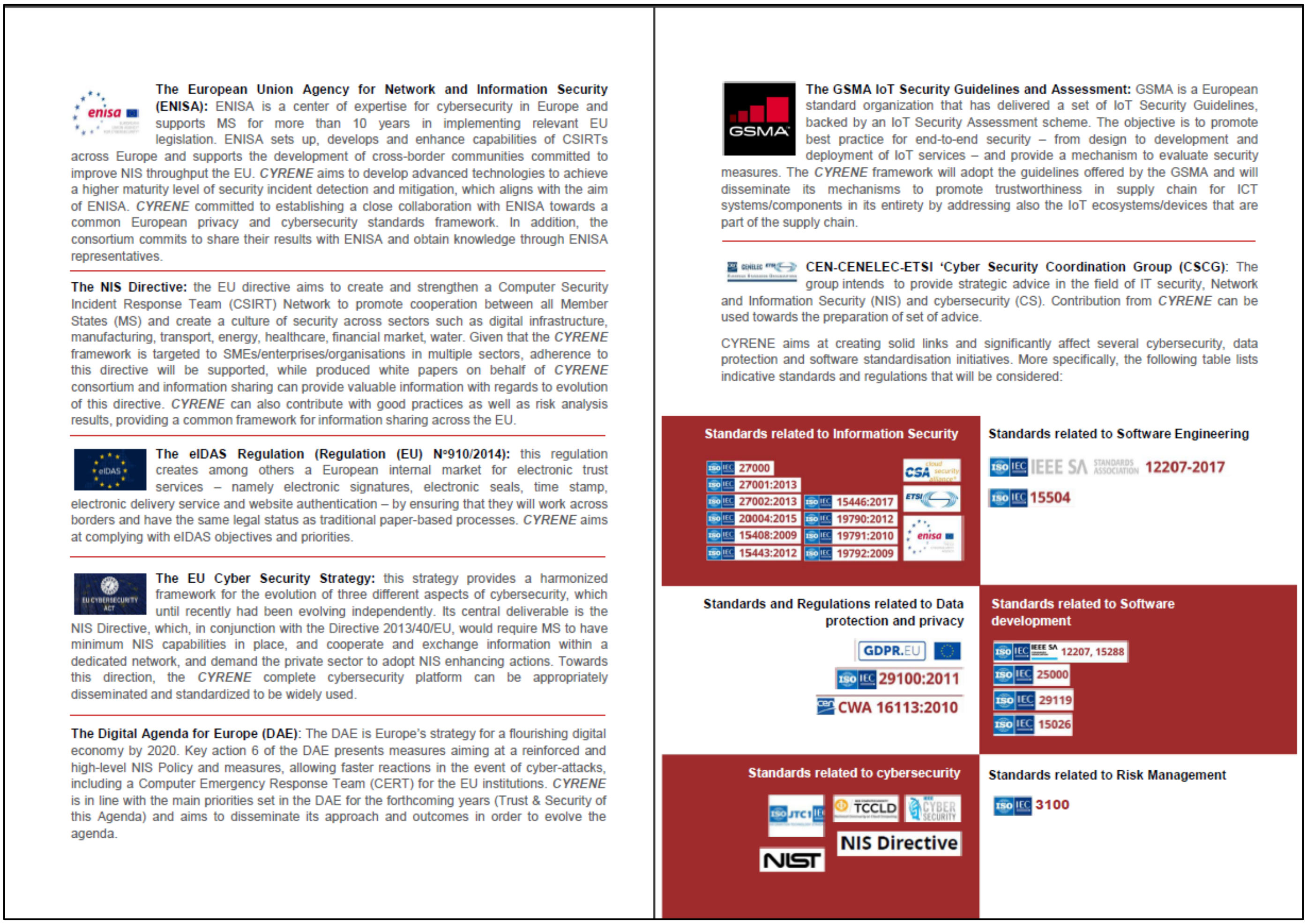
As referred to in the Grant Agreement (GA), CYRENE is responsible for producing the CYRENE's conformity/certification scheme that serves as the basis for Conformity Assessment Process (CAP). This implies a Security Certification Assessment Scheme for SCS for ensuring resilience and security, focusing on business-related aspects of SCS and built upon the ISO28001 standard. Also, an ICT Security Certification Assessment Scheme for ICT-based or ICT-interconnected SCS on certification of the supply chain IT infrastructure needs to be covered, built upon ISO standards 28001, 27001, and 27005. An ICT Security Certification Assessment Scheme for SCSs' IoT devices and Systems is also an important component, but it differs from existing schemes on individual IoT devices as more stress needs to be put on data protection and privacy issues. The European Cybersecurity Scheme (EUCC) and the European Cybersecurity Scheme for Cloud Services (EUCS), have been published after the CYRENE GA was signed, so the CYRENE consortium decided to utilize the EUCC to build the proposed SCS scheme as well as use the EUCS as an example, in order to ensure usability and usefulness of the project's work. CYRENE's EUSCS scheme is meant to define an approach that is compatible with EUCC but also incorporates the notion of the escalating vulnerability assessment level in bond with the different assurance levels. The CYRENE enhanced Risk and Conformity Assessment (RCA) methodology, can be utilised as for an enhanced risk assessment for the Supply Chain Service Provider (SCS-P) with the supply chain of business partners (SCS-Bps) to assess the SCS-risks, undertake controls and develop the protection profile (PP) of the SCS; and for a conformity assessment methodology where the assessors assess the conformance of the claims in the SCS Protection Profile (SCS-PP) to issue a SCS-certifyicate.

Conformity with existing standards

Standards of interest

Standards play a key role in improving cyber defence and cybersecurity across different geographical regions and communities. Standardizing processes are essential to achieve effective cooperation in cross-border, cross-community, and cross-sector environments. The number of standards development organizations and the number of published information security standards have increased in recent years, creating significant challenge. CYRENE has identified a set of standardization bodies and EU directives that must be closely monitored during the project lifetime, while in part of them, specific contributions are envisaged to be provided. A feasibility study of a security labelling is one of the tasks pursued within CYRENE. These bodies and announced strategies include:

Figure 3: Whitepaper (Page 3 of 5)



The European Union Agency for Network and Information Security (ENISA): ENISA is a center of expertise for cybersecurity in Europe and supports MS for more than 10 years in implementing relevant EU legislation. ENISA sets up, develops and enhance capabilities of CSIRTs across Europe and supports the development of cross-border communities committed to improve NIS throughput the EU. *CYRENE* aims to develop advanced technologies to achieve a higher maturity level of security incident detection and mitigation, which aligns with the aim of ENISA. *CYRENE* committed to establishing a close collaboration with ENISA towards a common European privacy and cybersecurity standards framework. In addition, the consortium commits to share their results with ENISA and obtain knowledge through ENISA representatives.

The NIS Directive: the EU directive aims to create and strengthen a Computer Security Incident Response Team (CSIRT) Network to promote cooperation between all Member States (MS) and create a culture of security across sectors such as digital infrastructure, manufacturing, transport, energy, healthcare, financial market, water. Given that the *CYRENE* framework is targeted to SMEs/enterprises/organisations in multiple sectors, adherence to this directive will be supported, while produced white papers on behalf of *CYRENE* consortium and information sharing can provide valuable information with regards to evolution of this directive. *CYRENE* can also contribute with good practices as well as risk analysis results, providing a common framework for information sharing across the EU.

The eIDAS Regulation (Regulation (EU) N°910/2014): this regulation creates among others a European internal market for electronic trust services – namely electronic signatures, electronic seals, time stamp, electronic delivery service and website authentication – by ensuring that they will work across borders and have the same legal status as traditional paper-based processes. *CYRENE* aims at complying with eIDAS objectives and priorities.

The EU Cyber Security Strategy: this strategy provides a harmonized framework for the evolution of three different aspects of cybersecurity, which until recently had been evolving independently. Its central deliverable is the NIS Directive, which, in conjunction with the Directive 2013/40/EU, would require MS to have minimum NIS capabilities in place, and cooperate and exchange information within a dedicated network, and demand the private sector to adopt NIS enhancing actions. Towards this direction, the *CYRENE* complete cybersecurity platform can be appropriately disseminated and standardized to be widely used.

The Digital Agenda for Europe (DAE): The DAE is Europe's strategy for a flourishing digital economy by 2020. Key action 6 of the DAE presents measures aiming at a reinforced and high-level NIS Policy and measures, allowing faster reactions in the event of cyber-attacks, including a Computer Emergency Response Team (CERT) for the EU institutions. *CYRENE* is in line with the main priorities set in the DAE for the forthcoming years (Trust & Security of this Agenda) and aims to disseminate its approach and outcomes in order to evolve the agenda.

The GSMA IoT Security Guidelines and Assessment: GSMA is a European standard organization that has delivered a set of IoT Security Guidelines, backed by an IoT Security Assessment scheme. The objective is to promote best practice for end-to-end security – from design to development and deployment of IoT services – and provide a mechanism to evaluate security measures. The *CYRENE* framework will adopt the guidelines offered by the GSMA and will disseminate its mechanisms to promote trustworthiness in supply chain for ICT systems/components in its entirety by addressing also the IoT ecosystems/devices that are part of the supply chain.

CEN-CENELEC-ETSI 'Cyber Security Coordination Group (CSCG): The group intends to provide strategic advice in the field of IT security, Network and Information Security (NIS) and cybersecurity (CS). Contribution from *CYRENE* can be used towards the preparation of set of advice.

CYRENE aims at creating solid links and significantly affect several cybersecurity, data protection and software standardisation initiatives. More specifically, the following table lists indicative standards and regulations that will be considered:

Standards related to Information Security

ISO IEC 27000
ISO IEC 27001:2013
ISO IEC 27002:2013
ISO IEC 20004:2015
ISO IEC 15408:2009
ISO IEC 15443:2012
ISO IEC 15446:2017
ISO IEC 19790:2012
ISO IEC 19791:2010
ISO IEC 19792:2009
CSA cloud security alliance
ETSI
enisa

Standards related to Software Engineering

ISO IEC IEEE SA STANDARDS ASSOCIATION 12207-2017
ISO IEC 15504

Standards and Regulations related to Data protection and privacy

GDPR.EU
ISO IEC 29100:2011
cen CWA 16113:2010

Standards related to Software development

ISO IEC IEEE SA 12207, 15288
ISO IEC 25000
ISO IEC 29119
ISO IEC 15026

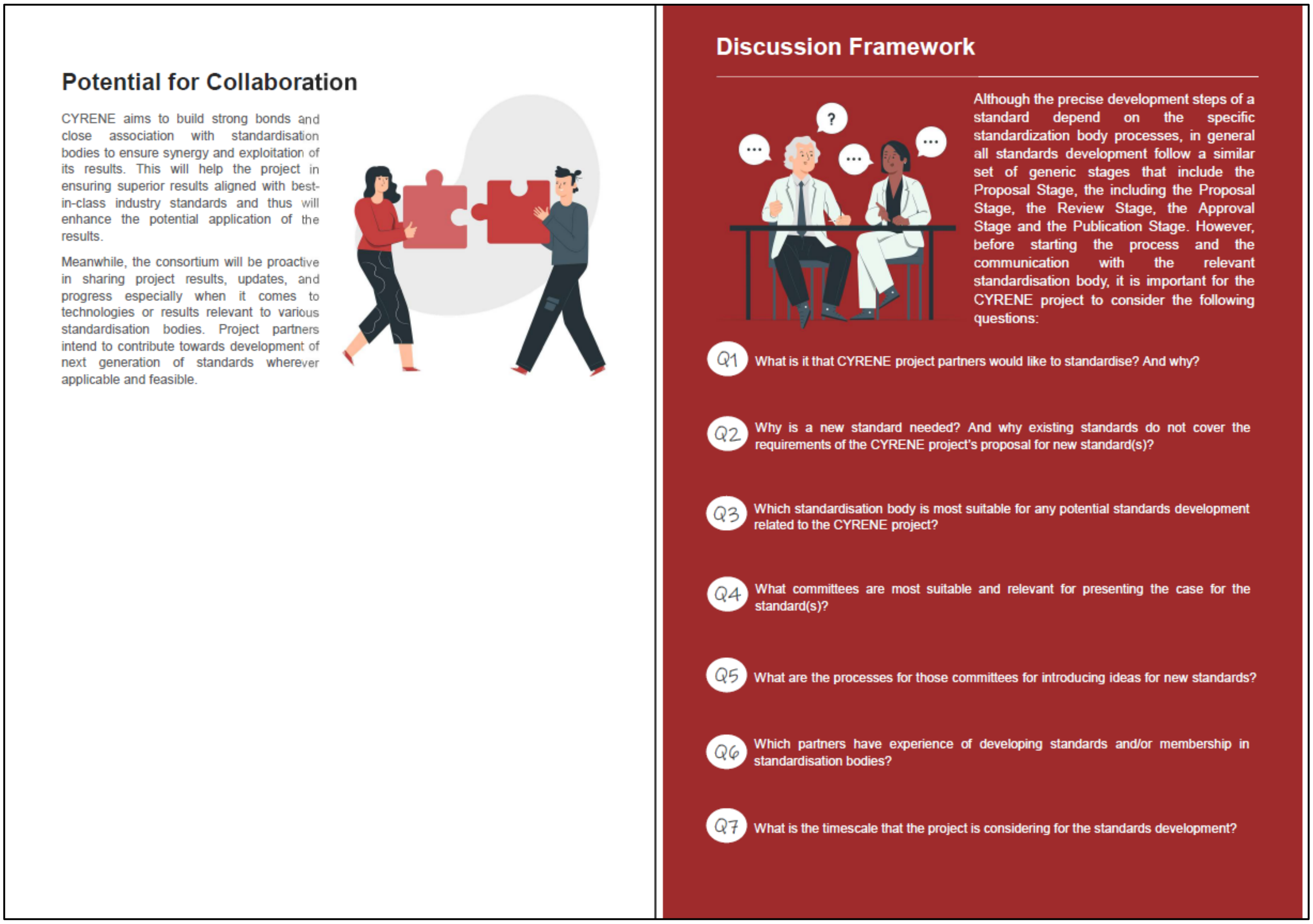
Standards related to cybersecurity

ISO JTC1 IEC
TCCLD
CYBER SECURITY
NIS Directive
NIST

Standards related to Risk Management

ISO IEC 3100

Figure 4: Whitepaper (Page 4 of 5)



Potential for Collaboration

CYRENE aims to build strong bonds and close association with standardisation bodies to ensure synergy and exploitation of its results. This will help the project in ensuring superior results aligned with best-in-class industry standards and thus will enhance the potential application of the results.

Meanwhile, the consortium will be proactive in sharing project results, updates, and progress especially when it comes to technologies or results relevant to various standardisation bodies. Project partners intend to contribute towards development of next generation of standards wherever applicable and feasible.

Discussion Framework

Although the precise development steps of a standard depend on the specific standardization body processes, in general all standards development follow a similar set of generic stages that include the Proposal Stage, the including the Proposal Stage, the Review Stage, the Approval Stage and the Publication Stage. However, before starting the process and the communication with the relevant standardisation body, it is important for the CYRENE project to consider the following questions:

Q1 What is it that CYRENE project partners would like to standardise? And why?

Q2 Why is a new standard needed? And why existing standards do not cover the requirements of the CYRENE project's proposal for new standard(s)?

Q3 Which standardisation body is most suitable for any potential standards development related to the CYRENE project?

Q4 What committees are most suitable and relevant for presenting the case for the standard(s)?

Q5 What are the processes for those committees for introducing ideas for new standards?

Q6 Which partners have experience of developing standards and/or membership in standardisation bodies?

Q7 What is the timescale that the project is considering for the standards development?

Figure 5: Whitepaper (Page 5 of 5)