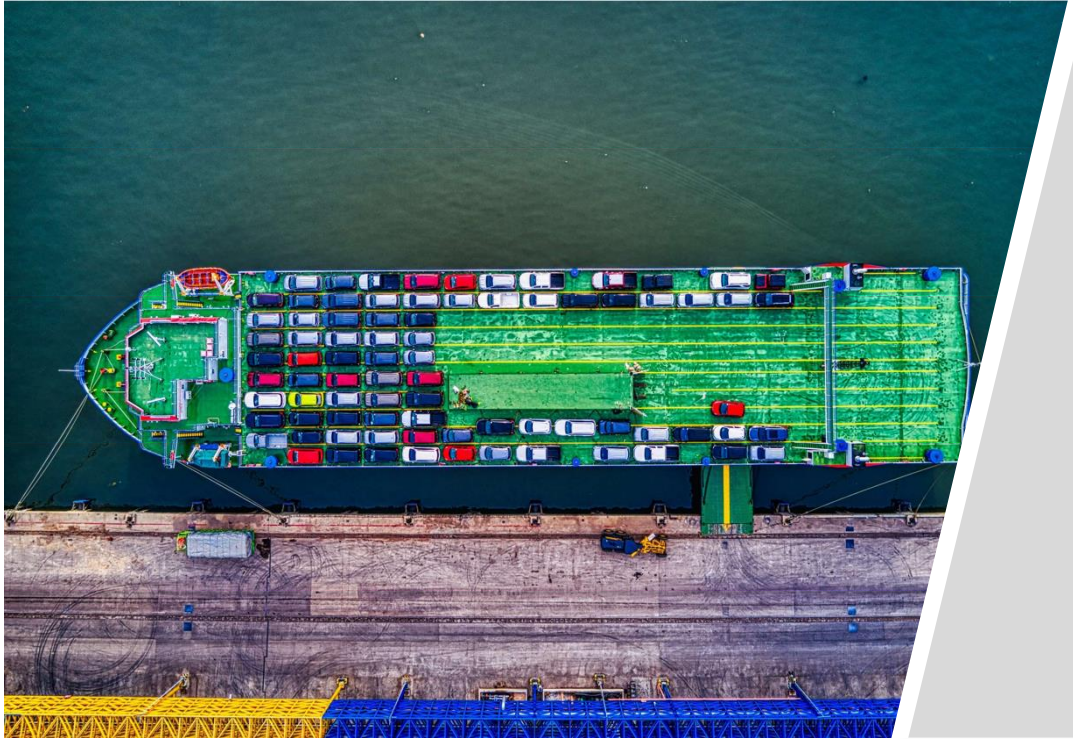


Contribution to Standardization

Certifying the Security and Resilience of Supply Chain Services

CYRENE White Paper 2023

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 selected 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.

About CYRENE

Global Supply Chains are a way of life for modern businesses, while they continuously become more complex and integrated. Organizations that participate in Supply Chains have become smarter, and they heavily depend on Information and Communication Technologies (ICT) they are also interconnected, by exchanging and sharing large amounts of data and involved in complex business processes. As the ICT infrastructures of involved stakeholders communicate in the open Internet environment, they are amenable to risks resulting from the 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 European 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 Risk and Conformity Assessment (RCA) Methodology for evaluating risks, 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 of European consumers to supply chains and their stakeholders, including providers and suppliers through formal certification of the resilience and security qualities of supply chain services contributing thus to a trusted 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

The CYRENE vision was to make key advances to the security, privacy, resilience, accountability, and trustworthiness of Supply Chain Services (SCSs) through the provision of a novel and dynamic Risk and Conformity Assessment (RCA) Methodology that evaluates the security supply chain services, the interconnected IT infrastructures that power them and devices they comprise. The main CYRENE outcomes are described below:

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

A novel Risk and Conformity Assessment (RCA) methodology has been proposed and supported by a platform and a toolset, enhancing the security of technologies that support SCs.

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

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

Services focused on dynamic forecast, detection and prevention of SC cyber security risks have been developed as well as mitigation strategies.

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.

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

An EU cybersecurity Certification Framework has been proposed through the collaboration with ENISA, ECSO, and national European Cybersecurity Centers of Excellence.

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 improves the operation of the European Single Market (ESM), the international business operations, and the quality of life through advanced and more safe services in the widespread domain of electronic services.

Relevant results for standardization

Main outcomes of CYRENE appropriate for standardization include:

1. The CYRENE glossary that connects interrelated terms from the risk and conformity assessment, especially security terms for the risk assessments (ISO2700x), supply chain security ISO2800x family of standards and the conformity assessment related standards (ISO 15408, ISO18045). The CYRENE glossary can be used to extend the ISO27000 glossary.
2. The proposed CYRENE cybersecurity certification schema for the supply chain services (EUSCS) is a main outcome that has been communicated to ENISA for further consideration and standardization efforts.
3. The dual use CYRENE risk/conformity assessment methodology is compliant with 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. The CYRENE methodology has already been communicated to ENISA and to ETSI (it was presented in the 2022 annual cybersecurity conference in Sophia Antipolis).
4. CYRENE proposed the development of an Information Security Management System (ISMS) for SCSs based on ISO2800x and ISO2700x. This online SCS-ISMS will be operated by the SCS provider in collaboration with its 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 if the controls implemented meet the corresponding security requirements. The CYRENE ISMS dedicated to the supply chains can be of interest to standardization bodies.
5. The CYRENE platform that can be used by the SC business partners to assess their SCS and develop its Protection Profile (PP) and by the auditors to assess the PP against the security requirements of the SCS scheme is an innovative tool that can be standardized by the technical oriented bodies (e.g. IEEE, OASIS, ETSI, CEN). The CYRENE platform has already been presented to IEEE conferences.

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 a comprehensive set of rules, technical requirements, standards, and procedures that are established at the Union level and apply to the certification or Conformity Assessment (CA) of specific ICT products. The CYRENE supply chain security certification scheme (EUSCS) used as template the European Cybersecurity Certification Scheme (EUCC) and was based upon the European scheme for cloud services (EUCS).

CYRENE EUSCS contributes to the certification of the cybersecurity of a SCS ecosystem and relies on ideas from different standards including the ISO/IEC 17065 standard in terms of applicable requirements to assessors performing certification, the ISO2700x ISO2800x series of standards and ISO/IEC 15408 standard. As stated 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 SCSs 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 SCSs 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 accordance with the different assurance levels. The CYRENE enhanced Risk and Conformity Assessment (RCA) methodology, can be utilised as 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 theSCS; and as a conformity assessment methodology where the assessors evaluate the conformance of the claims in the SCS Protection Profile (SCS-PP) to issue a SCS-certificate.

Conformity with existing standards

Standards of interest

Standards play a key role in improving cyber defense 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 have been closely monitored during the project lifetime, and for some of them, specific contributions have been provided. A feasibility study of a security labelling is one of the tasks pursued within CYRENE. These bodies and adopted strategies include:

The European Union Agency for Network and Information Security (ENISA): ENISA is a European center of expertise in cybersecurity and supports Member States 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. ENISA is the responsible EC agency to implement the Cybersecurity Act. ENISA has already proposed the EUCC and EUCS, where the 5G scheme is under preparation. ***CYRENE*** already delivered to ENISA the developed CYRENE Risk and Conformity Assessment methodology (CYRENE-RCA) and the CYRENE-EUSCS scheme.

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 considered the guidelines offered by the GSMA.

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.

Given that CYRENE aims to secure supply chain services (a main challenge in all economic sectors), CYRENE highly contributes in a numerous of EU directives including:

The NIS and NISII Directives creates a culture of security across sectors such as digital infrastructure, manufacturing, transport, energy, healthcare, financial market, water. NISII goes a step further and aims to secure the supply chains and requires additional mitigation actions to supply chain providers,

---

The EU Cybersecurity Act establishes a cybersecurity certification framework for ICT products and services (including supply chain services) that provides EU-wide certification schemes as a comprehensive set of rules, technical requirements, standards, and procedures. This way it will be possible to ensure the public trust in the cybersecurity of IT products and services. It is important that it can be shown that a product has been checked and certified to conform to high cybersecurity standards.

The **General Data Protection Regulation (GDPR)** sets data protection rules explaining what, how, and when people can access information about them and provides constraints on what organisations can do with personal data.

The New Legislative Framework (NLF) improves market surveillance, introduces rules to better protect both consumers and professionals from unsafe products (EU or non-EU), sets rules for the accreditation, establishes a common legal framework for industrial products.

The Cyber Resilience Act will set new cybersecurity rules in due time for digital products and ancillary services. This initiative will promote the security of supply chain services as well since it aims to address market needs and protect consumers from insecure services by introducing common cybersecurity rules for manufacturers and vendors of tangible and intangible digital products.

Digital Services Act provides security and privacy obligations and restrictions not only to large platform-based service providers (e.g. Google, Facebook) but to all service providers (including supply chain providers).

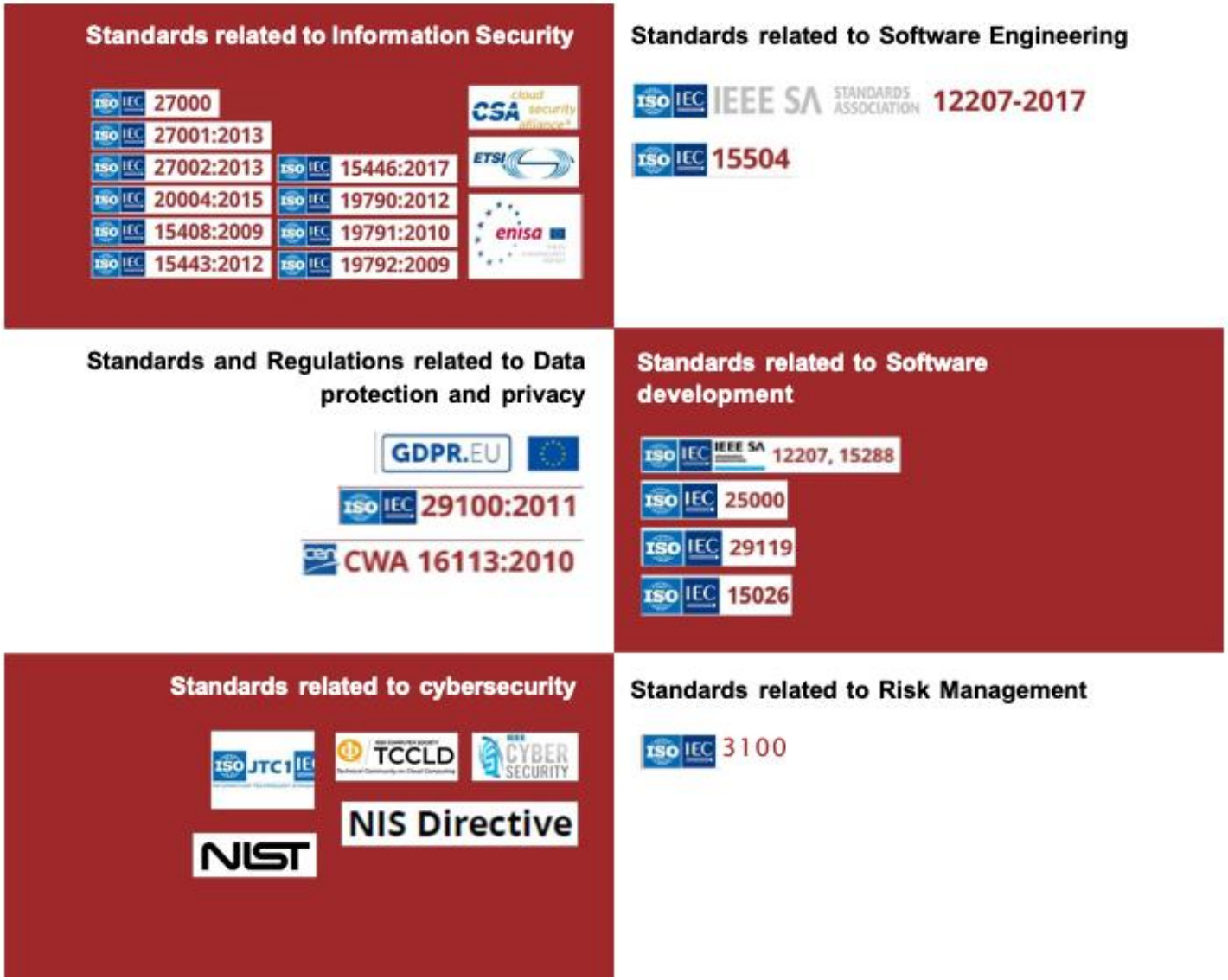
The eIDAS Regulation (Regulation (EU) Nº910/2014): this regulation creates among others a European internal market for electronic trust services – namely electronic signatures, electronic seals, time stamp, electronic delivery service and website authentication – by ensuring that they will work across borders and have the same legal status as traditional paper-based processes.

CYRENE contributes to the implementation of EU cybersecurity strategies including:

The EU Cyber Security Strategy aims to ensure a global and open Internet with strong safeguards where there are risks to security and the fundamental rights of people in Europe; it contains concrete proposals for deploying three principal instruments: regulatory, investment and policy initiatives which will address three areas of EU action: resilience, technological sovereignty and leadership; operational capacity to prevent, deter and respond; cooperation to advance a global and open cyberspace.

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 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 have been considered:



Collaboration

CYRENE partners participate in various standardization bodies and have built strong bonds with stakeholders This heled the project in ensuring superior results aligned with best-in-class industry standards and thus enhanced the potential application of the results.

Meanwhile, the consortium will continue in sharing project results, updates, and progress especially when it comes to technologies or results relevant to various standardisation bodies. Project partners intend to continue contributing for the 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 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?