CYRENE

# Contribution to Standardization

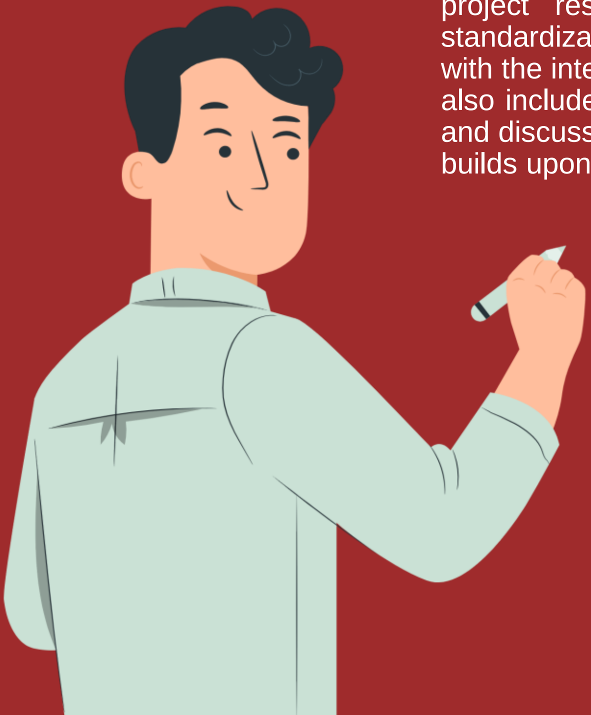
## Certifying the Security and Resilience of Supply Chain Services

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.



# 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.

# Relevant results for standardisation

**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:

**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 THE EU CYBERSECURITY AGENCY

### 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 STANDARDS ASSOCIATION 12207, 15288
- ISO IEC 25000
- ISO IEC 29119
- ISO IEC 15026

### Standards related to cybersecurity

- ISO JTC1 IEC INFORMATION TECHNOLOGY STANDA
- IEEE COMPUTER SOCIETY TCCLD Technical Community on Cloud Computing
- IEEE CYBER SECURITY
- NIS Directive
- NIST

### Standards related to Risk Management

- ISO IEC 3100

# 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?

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.