



# CYBER RESILIENCE FOR SUPPLY CHAIN OPERATIONS:

INSIGHTS FROM THE  
CYRENE STANDARDISATION  
WORKSHOP 2023



# Introduction

Welcome to the CYRENE Standardisation Workshop booklet, a comprehensive source of information about this pivotal event in our project's journey. The EU-funded CYRENE project, an endeavour aimed at fortifying the security and resilience of ICT-supported supply chain services, recognises the critical role that standardisation plays in achieving its objectives in line with the European Cybersecurity Act.

The CYRENE Standardisation Workshop, held in July 2023, served as a crucial platform to bring together stakeholders, experts, and consortium partners, facilitating insightful discussions around cybersecurity in supply chains. The workshop's primary objective was to foster understanding, exchange knowledge, and develop cooperative strategies around the development of standardisation norms.

In this booklet, we shed light on the intricate details of the workshop, its key takeaways, speakers' contributions, and how it serves to reinforce CYRENE's commitment to enhancing cybersecurity resilience in supply chain services. Whether you're a participant seeking to reflect on the experiences and learnings of the workshop, or an interested party aiming to understand the conversations and outcomes, this booklet serves as your comprehensive guide.

We are pleased to share the insights, discussions, and initiatives that emerged from this gathering. Let's delve into the details of the CYRENE Standardisation Workshop.



# Detailed Workshop Schedule and Agenda

The CYRENE Standardisation Workshop was a day-long event that took place on June 16, 2023. The schedule was strategically designed to maximize knowledge exchange and productive discussions.

Time (CET)	Title	Presented by
10:00 - 10:10	Welcome	PN
10:10 - 10:40	CYRENE Methodology and Standardization (30min)	MAG/UBI
10:40 - 11:10	Standardisation supporting EU legislation	ENISA
11:10 - 11:30	Coffee Break	
11:30 - 12:00	ETSI Cybersecurity Work on Cyber Resiliency and Supply Chain Management, including the Zero Trust Model	ETSI
12:00 - 12:30	Security standardisation by CEN & CENELEC	CEN CENELEC
12:30 - 13:00	ISO/IEC 27001 and 27002 and conformity assessment in the context of supply chain security	ISO
	Lunch Break	
14:00 - 14:30	Overview of ISO/IEC 27036 "cybersecurity security in supplier relationships"	ISO
14:30 - 14:45	BIECO approach for a certification of cybersecurity systems	BIECO
15:00 - 15:15	Standardization Pillars Supporting the Automation of Cloud Security Certification "the H2020 MEDINA project"	MEDINA
15:15 - 15:30	IETF Standardization of Lightweight Security Protocols for the IoT	SIFIS HOME
15:30 - 15:45	Guidance on Trusted Environments for Creating Cyber Resilient Devices	ASSURED
15:45 - 16:00	Strengthening IoT Security: Insights from the IoTAC Project	IOTAC
16:00 - 16:15	Standardization activities in European research projects: Case of H2020 SANCUS	SANCUS
16:15 - 16:45	Round table discussion	ALL
16:45 - 17:00	Closing	MAG, ALL



# Introducing the Speakers: Insights and Expertise

This section of the booklet aims to introduce you to the exceptional individuals who presented at the CYRENE Standardisation Workshop, elaborating on their roles in the project, their professional expertise, and the valuable insights they shared.



# Standardisation Bodies



Dr. Edward Humphrey from ISO is the convenor of ISO/IEC JTC 1/SC 27/WG 1, the working group responsible for the ISO/IEC 27000 family of standards. Edward has over forty years experience working in the field of security including advising international organizations, governments and various EU institutions



Mrs. Nadya Bartol from ISO is a managing director at Boston Consulting Group, where she leads cyber and digital risk practice in North America. Nadya has worked with NIST and within ISO for a long time on the topics of cybersecurity, cyber supply chain risk management, and security measurement.



Mr. Slawomir Gorniak from ENISA is a telecommunications engineer focused on network security. Since 2008 he works at ENISA (EU Agency for Cybersecurity), where he has been involved in the areas of standardisation, certification and electronic identification. He is a coordinator and co-author of multiple ENISA reports covering various aspects of information security.



Mr. Tony Rutkowski from ETSI is an engineer-lawyer with an extremely diverse, sixty-year professional career spanning the telecommunication, mobile, internet, satellite, and broadcasting fields in the U.S. and Europe where he has shaped major technical and legal developments in senior governmental, company, and academic leadership positions at international, national, and local levels



Mr. Pertti Woitsch from CEN CENELEC is an experienced defence & security industry professional with wide experience in international sales, marketing and business development. He currently works as CEO at Woitsch Consulting Oy, a Helsinki based advisory firm with focus on providing consulting services to the industry, national public authorities and the research community, including EU-funded research projects.



## Projects



Mr. Jose Barata from BIECO project is a Full Professor at the Electrical and Computing Engineering, Member of the Scientific Committee of the Doctoral Program in Electrical and Computing Engineering at the NOVA-FCT, where he is currently responsible for the courses units Robotics, Systems Integration, Telerobotics and Autonomous Systems, and Robotics Systems and CIM.



Dr. Jesus Luna Garcia from MEDINA project is the technical manager of the EU-funded MEDINA project on automated certification. He has worked since 1995 in the field of cybersecurity, both in America and Europe. He holds a PhD degree in Computer Architecture from the "Technical University of Catalonia" (Spain), and has co-authored more than 50 cybersecurity-related publications including scientific papers, standards, and a patent.



Dr. Marco Tiloca from SIFIS HOME is currently a Senior Researcher in the Cybersecurity Unit of RISE Research Institutes of Sweden in Stockholm (Sweden). His research interests are in the field of network and communication security, and include security in the Internet of Things, secure group communication, key management, and access control.



Dr. Dimitris Karras from ASSURED project is a Research Associate at the Digital Security and Trusted Computing Department of UBITECH. He has received his PhD in Physical Layer Security, as well as his degree in Electrical Engineering and Computer Science, from the Aristotle University of Thessaloniki.



Dr. Marija Jankovic and Mr. Sascha Hackel from IOATC project: Dr. Marija is a senior research associate at the Information Technologies Institute of the Centre for Research and Technology Hellas (CERTH), holding B.Sc., M.Sc., and Ph.D. degrees in Information Systems from the University of Belgrade, Faculty of Organizational Sciences. Mr. Sascha is a research associate at the Fraunhofer Institute for Open Communication Systems (FOKUS) in Berlin. As a member of the System Quality Competence Center, he is involved and responsible for validation and test projects on next generation networks and software technologies



Dr. Wissam Mallouli from SANCUS project is currently the Chief Technology Officer (CTO) at Montimage, an SME based in Paris, France. He obtained his Telecommunication Engineer degree from the National Institute of Telecommunication (INT) in 2005

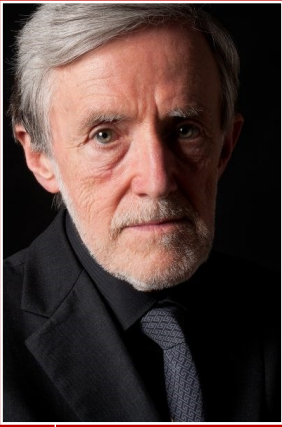


# Journey Through the Sessions: Enlightening Conversations Unpacked

This section outlines the topics discussed during each session, highlighting the key points and any conclusions or next steps.



# Standardisation Bodies



## ISO/IEC 27001 and 27002 and conformity assessment in the context of supply chain security

Dr. Edward Humphrey provided an overview of supply chain security as included in ISO/IEC 27001 and ISO/IEC 27002. He showed the relationship between these standards and ISO 28001, followed by presentation of conformity assessment, and certification in particular, in the context of ISO/IEC 27001.



## Overview of ISO/IEC 27036 – cybersecurity security in supplier relationships

Mrs. Nadya Bartol presented an overview of ISO/IEC 27036 including target audiences, structure of this multipart standard, and its contents. She further discussed how to use the standard to manage cyber and information security aspects of any supplier relationship, acquiring and managing digital products and services, as well as acquiring and managing cloud-based services.

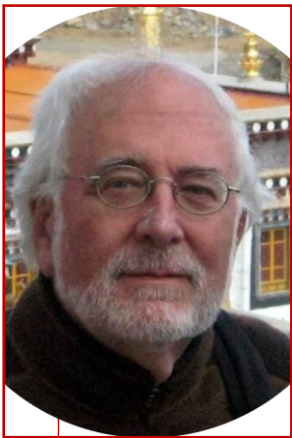






## Standardisation supporting EU legislation

Mr. Slawomir Gorniak reviewed the current situation on proposed legislative acts related to cybersecurity by the European Commission. He presented how ENISA plays a crucial role in strengthening cybersecurity across the European Union. Its mandate is comprehensive and solid, extending to numerous important tasks that include, but aren't limited to, the preparation of draft cybersecurity certification schemes and standardisation. ENISA has an unwavering commitment to enhancing capacity building and preparedness across the Union, offering support in the development of coordinated responses to large-scale cyber incidents and crises



## ETSI Cybersecurity Work on Cyber Resiliency and Supply Chain Management, including the Zero Trust Model

Mr. Tony Rutkowski addressed cyber resiliency throughout the supply chain and the various related frameworks and measures using risk-based, system of trust, and zero trust approaches, including the proposed EU Cyber Resilience Act. The cyber resiliency approaches taken in existing EU legislation are exemplary of legacy “Common Criteria” certification programmes that proved ineffective, enormously costly and impossible to implement among the national security communities. He further discussed the Cyber Vulnerability Disclosure Ecosystem, explaining its value, timeline, participants, and challenges, concluding that the ecosystem is especially daunting for SMEs and general public.





## Security standardisation by CEN & CENELEC

Mr. Pertti Woitsch discussed cyber resiliency throughout the supply chain and the various related frameworks and measures using risk-based, system of trust, and zero trust approaches, including the proposed EU Cyber Resilience Act.

All presentations provided by Standardisation bodies are available at the CYRENE website [here](#)



# Projects



## BIECO approach for a certification of cybersecurity systems

Jose Barata presented BIECO's approach to certification of cybersecurity systems, and their integration within the BIECO ecosystem



## Standardization Pillars Supporting the Automation of Cloud Security Certification – the H2020 MEDINA Project

Jesus Luna Garcia discussed the standardization challenges faced by the MEDINA project in leveraging automated cybersecurity certification for cloud services.





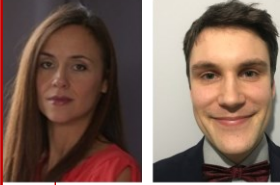
## IETF Standardization of Lightweight Security Protocols for the IoT

Marco Tiloca overviewed the standardization contributions from the SIFIS-Home project in the development of lightweight security protocols for IoT.



## Guidance on Trusted Environments for Creating Cyber Resilient Devices

Dimitris Karras discussed the guidance on trusted environments for creating cyber-resilient devices and the role of the ASSURED project



## Strengthening IoT Security: Insights from the IoTAC Project

Marija Jankovic and Sascha Hackel explored the security testing approaches implemented in the IoTAC project and the project's multi-layered security approach



## Standardization activities in European research projects: Case of H2020 SANCUS

Wissam Mallouli from SANCUS shared the project's activities in ensuring the security of 5G networks, in compliance with the current ICT and network security standards


All presentations provided by  
Projects are available at the  
CYRENE website [here](#)




# Nuggets of Wisdom: Pivotal Insights & Takeaways from the Workshop




# The key takeaways from this workshop include:




The relevance of standardization for cyber-physical systems, as echoed across the presentations of all the speakers.




The realization of how standardization can help in achieving the goals of the CYRENE project.



Insights into the current state and future plans of security-related standards from various standardisation bodies like ETSI, ISO/IEC, IEEE, ENISA, and CEN-CENELEC



Understandings gained from the approaches, methodologies, and standard-compliant solutions developed by various EU-funded projects, in the quest for securing their respective domains.



The potential implications of the various projects' approaches for standardization in the broader field of cybersecurity, which can impact and shape future industry standards

