ECSO activities in support of the EU Cybersecurity Act

Dr. Roberto G. Cascella

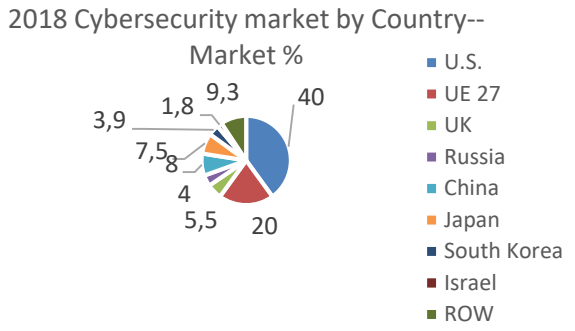
ECSO Secretariat

Cybersecurity Standardization Conference 2021

– Online, 4 February 2021 –

Market and geopolitical environment

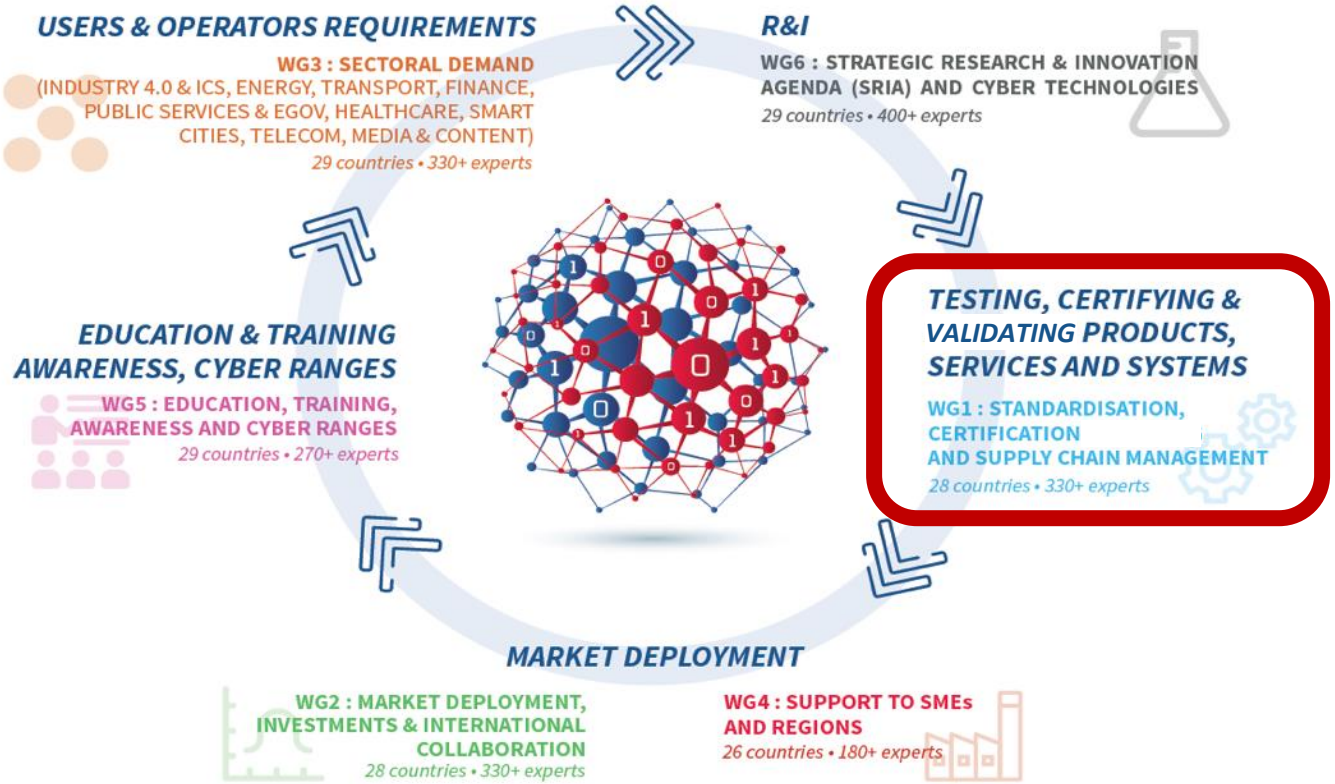
- **Global cybersecurity market** (estimation: ECSO 2018 market analysis): 115 bln € / Market growth rate + 13% by 2022.
- Market dominated by **global suppliers** from North America and Asia: most of the IT hardware and software products are manufactured outside the European Union
- **EU market** about 25 bln € composed by about 12K supplier companies (74% of them are Micro and SMEs).
- **EU public procurement** still leveraging upon non-EU solutions, even for sensitive issues.
- Growing "**sovereignty**" issue (in particular after the COVID with digital transformation)



Sources: Momentum Partners, Visiogain 2018-2028 Market Report

There is innovation in Europe,
but still fragmented markets

ECSO Working Groups (WG) collaborating with each other: Cybersecurity 360°



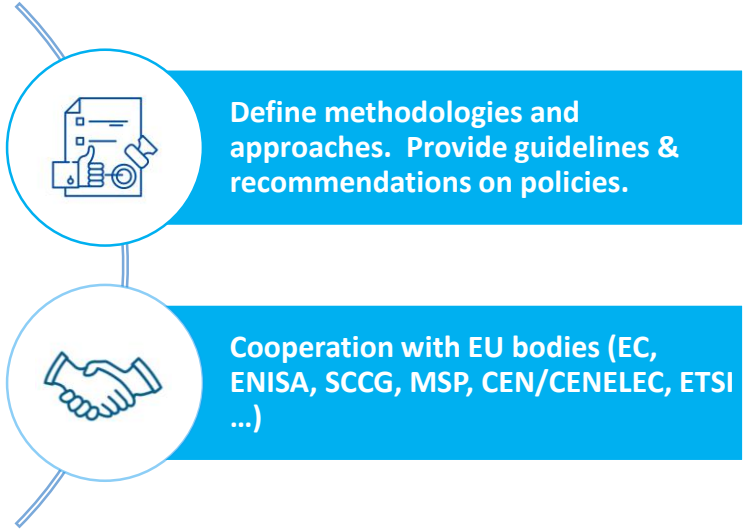
WG1

Standardisation, Certification, and Supply Chain Management

Support the roll-out of EU ICT security certification schemes,

standard and legislation recommendations (MoU with ETSI, CEN/CENELEC, collaboration with EC, ENISA and JRC, member of the SCCG)

and the establishment of trusted supply chains.



Connected Components

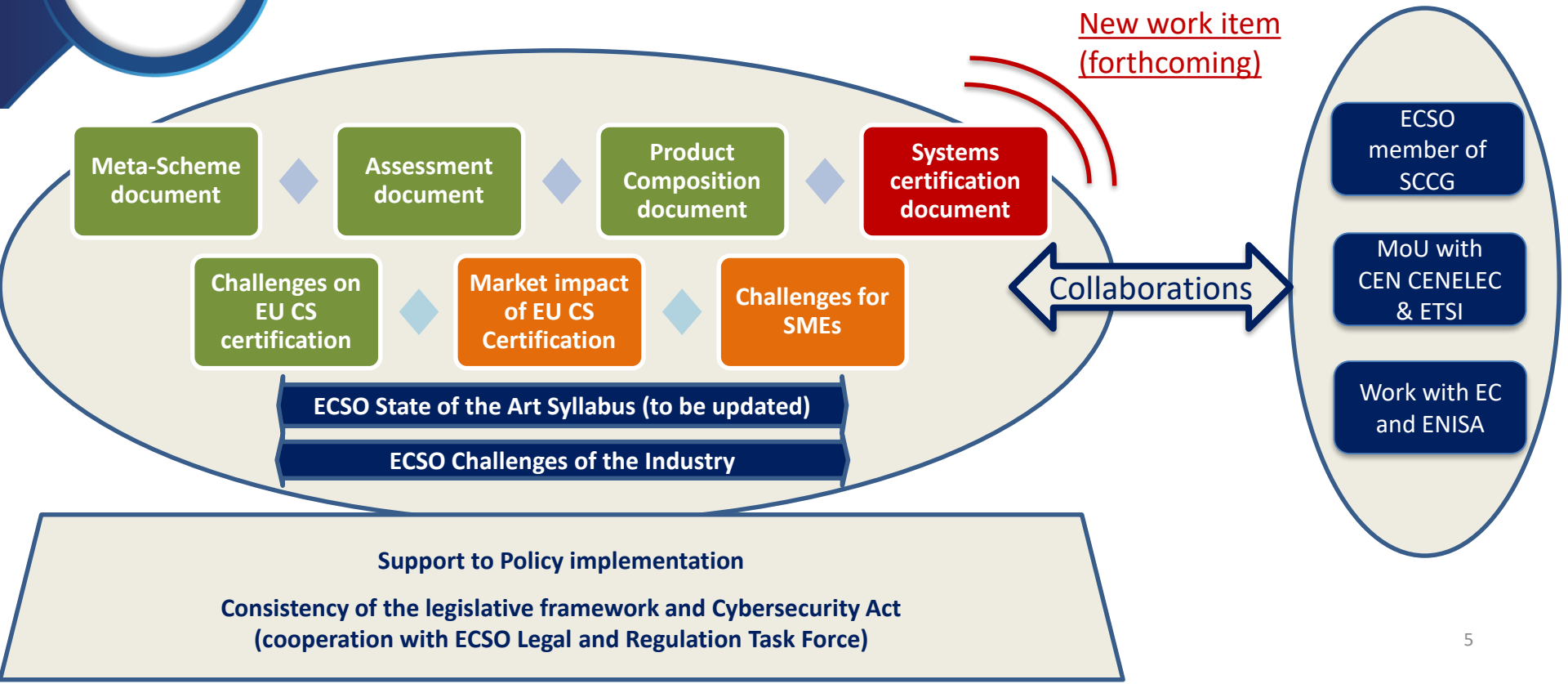
Work on the inter-relationship (“composition”) of EU scheme certified components based on standards for trusted supply chain and product certification in line with to the EU Cyber Act.

Digital Services and Systems

Understand the systems’ & services’ dependencies, needs and current approaches for risk management and operational aspects

Cybersecurity ecosystem: stakeholders, market and regulations

WG1 – Standardisation, Certification, and Supply Chain Management



The value of certification: important factors

- Digital transformation and increase reliance on new technologies
- Trusted supply chain to ensure business and service resilience
- Build trust via future European cybersecurity certification schemes across industries
  - Encourage, define, monitor, assess and help companies improving the overall security of their products
  - Calibrate security controls according to the risk-based assessment
  - Horizontal schemes to support sector specific needs
- Whole lifecycle, management of vulnerabilities and risk, etc.
  - Assessment of the security claims according to the desired assurance level
  - Surveillance of certified products and certificate validity lifecycle

Areas of interest for future certification

- Some areas highlighted by ECSO members are:
  - SDL/Secure Development Lifecycle process
  - 5G Component, product (SW, HW), systems and services
  - Industrial and consumer IoT devices
  - Healthcare devices, services, organisations
  - Industrial environments
  - Smart Buildings
  - Critical infrastructure and ICS/SCADA devices

CONTACT US!

European Cyber Security Organisation
29, Rue Ducale
1000 – Brussels – BELGIUM

E-mail:
secretariat@ecs-org.eu

Follow us:

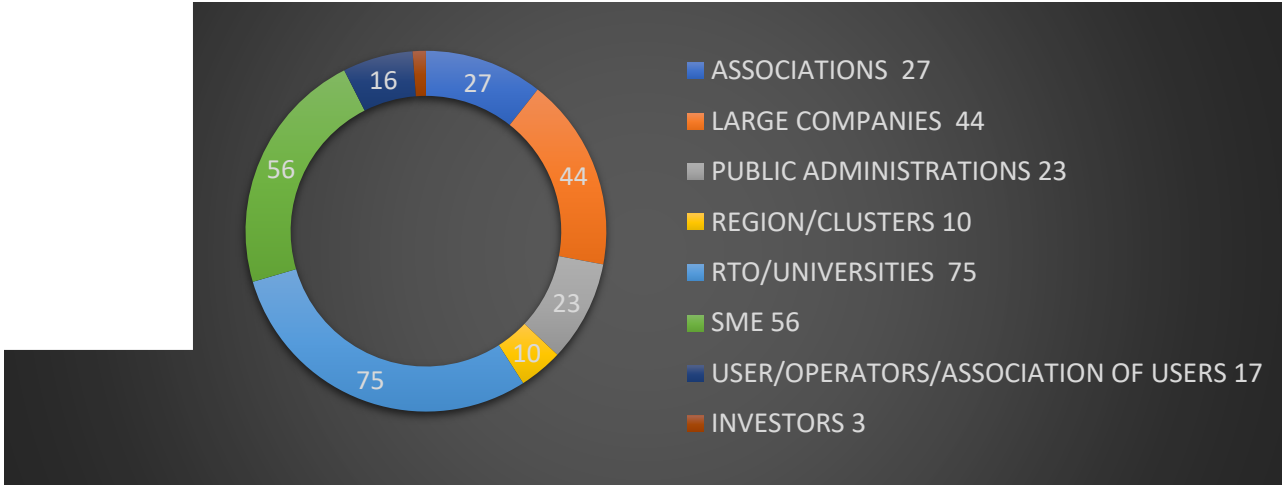
www.ecs-org.eu

LinkedIn: https://www.linkedin.com/company/ecso-cyber-security/

Twitter: @ecso_eu

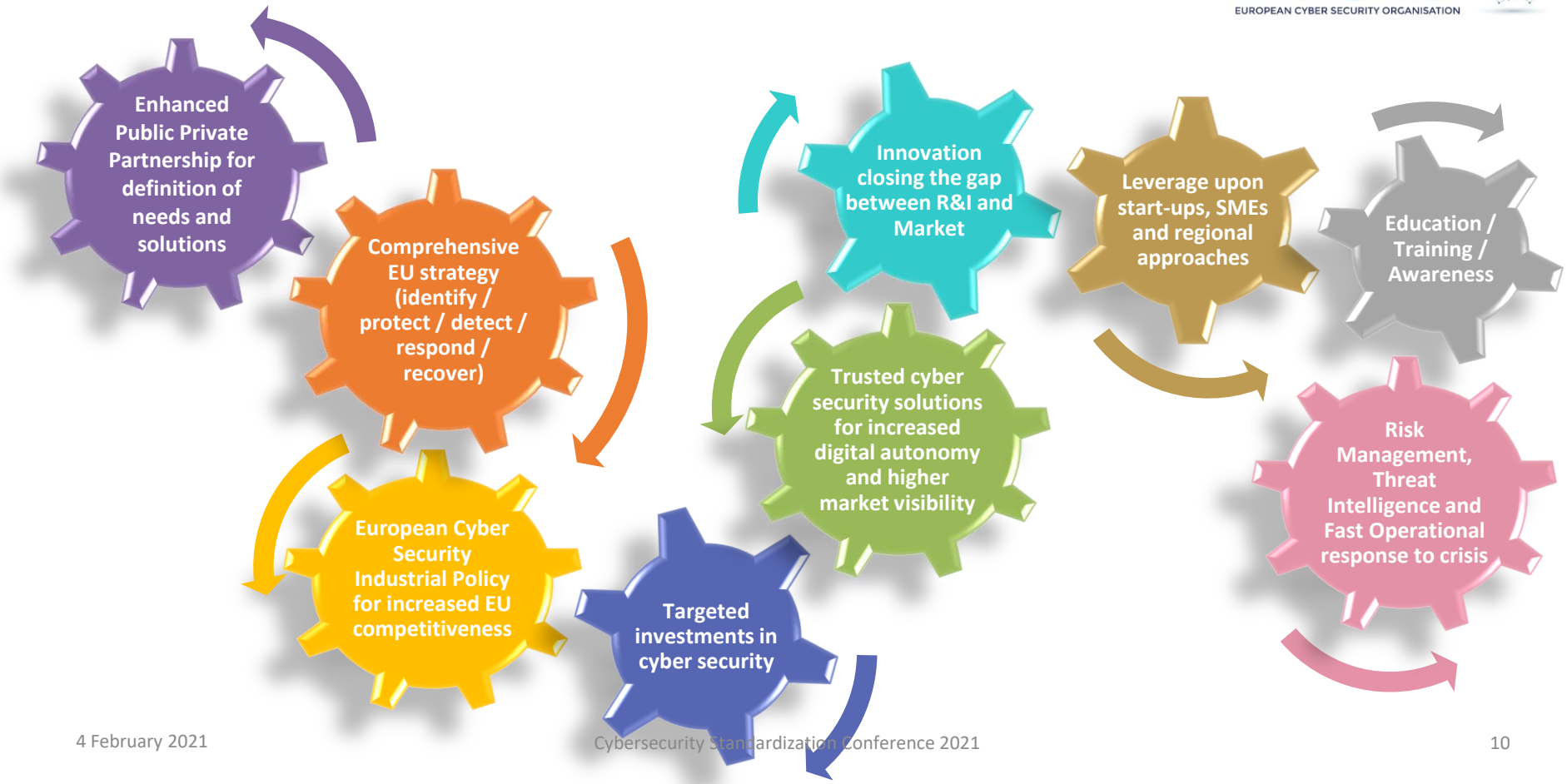
European Cyber Security Organisation

Established in 2016 for the implementation of the contractual Public-Private Partnership (cPPP) on cyber security with the European Commission



Our membership has grown from 132 members in June 2016
to 255 members across 29 countries in January 2021, connecting more than 2000 organisations in Europe

Since 2016 ECSO has been addressing several building blocks through its Working Groups

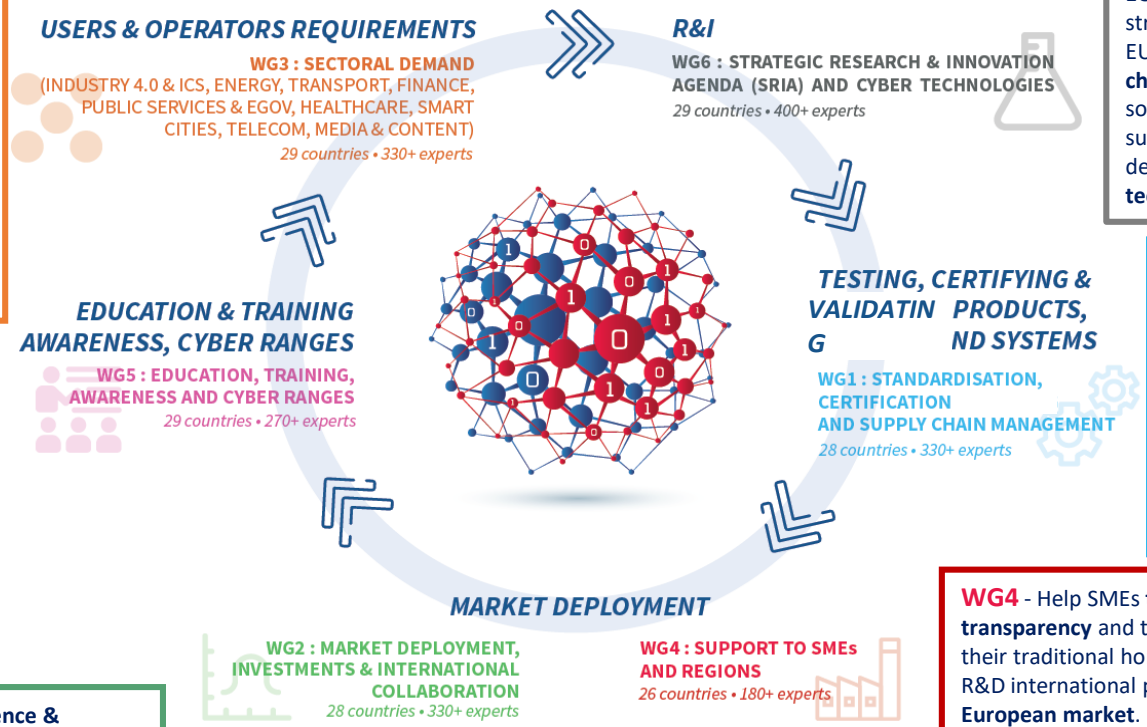


ECSO Working Groups (WG) collaborating with each other: Cybersecurity 360°

WG3 - Engage directly with users (operators, companies, governments) to **understand cyber threats, share information among trusted peers**, **link supply and demand,** and act as a **transversal WG that defines needs of the sectors** for standardisation / certification; education, training and exercises; research / technologies; local / regional initiatives.

WG5 - Contribute towards a cyber security **competences and capacity building effort** for the European digital agenda, through increased **education, professional training and skills development**, as well as actions on **awareness-raising** and **gender inclusiveness**.

WG2 - Provide **market intelligence & qualitative analysis**, facilitate the **visibility of European solutions** across Europe and beyond, and boost the level of private **investments** in cybersecurity market and its solutions.



WG6 - Define the cyber security **EU R&I roadmap and vision** to strengthen and build a resilient EU ecosystem. Analyse the **challenges of digitalisation** of the society and industrial sectors to sustain EU **digital autonomy** by developing and fostering **trusted technologies.**

WG1 - Support the roll-out of **EU ICT security certification schemes, standard and legislation recommendations** (MoU with ETSI, CEN/CENELEC, collaboration with EC, ENISA and JRC, member of the SCCG) and the **establishment of trusted supply chains**.

WG4 - Help SMEs **to create more market transparency** and to reach out far beyond their traditional home markets to partner in R&D international project and to **access European market**.

Engage with Regions specialised in cybersecurity to support the implementation of an innovative Smart Commercialisation Strategy

WG1 already available work

To foster trust in digitalization and promote innovation

ECSO Meta-Scheme Approach helps to harmonise minimum security requirements, define a unified levelling across verticals, and provide a common way to define required security claim

- https://www.ecs-org.eu/documents/publications/5a3112ec2c891.pdf

It can act as a methodological tool to structure the landscape, "glue" together the existing schemes and specify additional steps

ECSO Assessment options explains how to benefit from the right mix of security assessments, and what constraints to be aware of

- https://www.ecs-org.eu/documents/publications/5d6fbbd00cfe7.pdf

It provides insights to organisations that are building their cybersecurity capabilities and need to choose how to assess security

ECSO State of the Art Syllabus gives an overview of existing certification schemes & standards: products & components; ICT services; Systems; Vertical Sectors; etc.

- https://www.ecs-org.eu/documents/publications/5a31129ea8e97.pdf

It provides a cartography in standardization – currently under revision – new version coming soon!

ECSO Product Certification Composition addresses composition in an agnostic way with respect to standards and certification schemes to create an environment favourable for re-use of certification evidence

- https://ecs-org.eu/documents/publications/5fbfc8436e5a1.pdf

It provides guidelines and structure how to proceed when seeking a certification by composition under the requirements defined by EU Cybersecurity Act

ECSO challenges for the roll-out of the Cybersecurity Act focuses on how to achieve framework consistency, what is intended for composition and the related challenges for a system integrator, and on the areas of interest for future priorities

- https://ecs-org.eu/documents/publications/5fd787e5cae1c.pdf

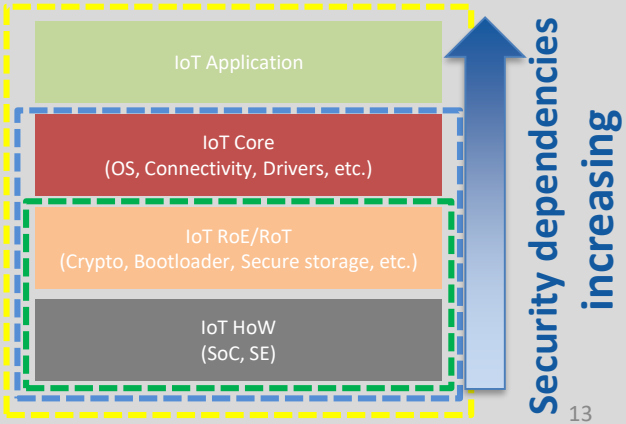
It discusses the aspects that could hinder the usage of future European cybersecurity certification schemes across industries

ECSO Product Certification Composition

Available at https://ecs-org.eu/documents/publications/5fbfc8436e5a1.pdf

- **Enable** efficient **re-use** of **certificates** and **evaluation evidence**
- **Decrease** certification **cost** and **improve** overall process **speed**
- Benefit horizontal components **specialised in application** domains
- Strongly **contribute** on the **time to market** of certified products

- **Composition document** – underlying principles and practical aspects
- Initial considerations for composition:
  - Bottom-up, top-down, mix
  - Within the **same** scheme (standard) or **multiple** schemes
  - Component tightly **integrated** or **independent**
- **Guidelines** for certification composition and steps
- Component certification elements that might be necessary for **assessment**



WG1

Standardisation, Certification, and Supply Chain Management

OBJECTIVES 2021

- Extend the composition across EU schemes, focus on the technical details of the composition approach: the operational phase (e.g. vulnerability and patch management) of the composed product and expectations for product composition. Link with first EU certification schemes.
- Study secure system and service lifecycle and associated risk management and certification.
- Identify the challenges for SMEs in using certification schemes and define guidelines / best practices.
- Address the challenges for a trusted supply chain and management of the risks.
- Support policies implementation: link with DEP priorities describing challenges and plan for the future. Development of capabilities.
- Continue the collaboration with ENISA, EC, European SDOs and other relevant stakeholders.

Cybersecurity ecosystem: stakeholders, market and regulations