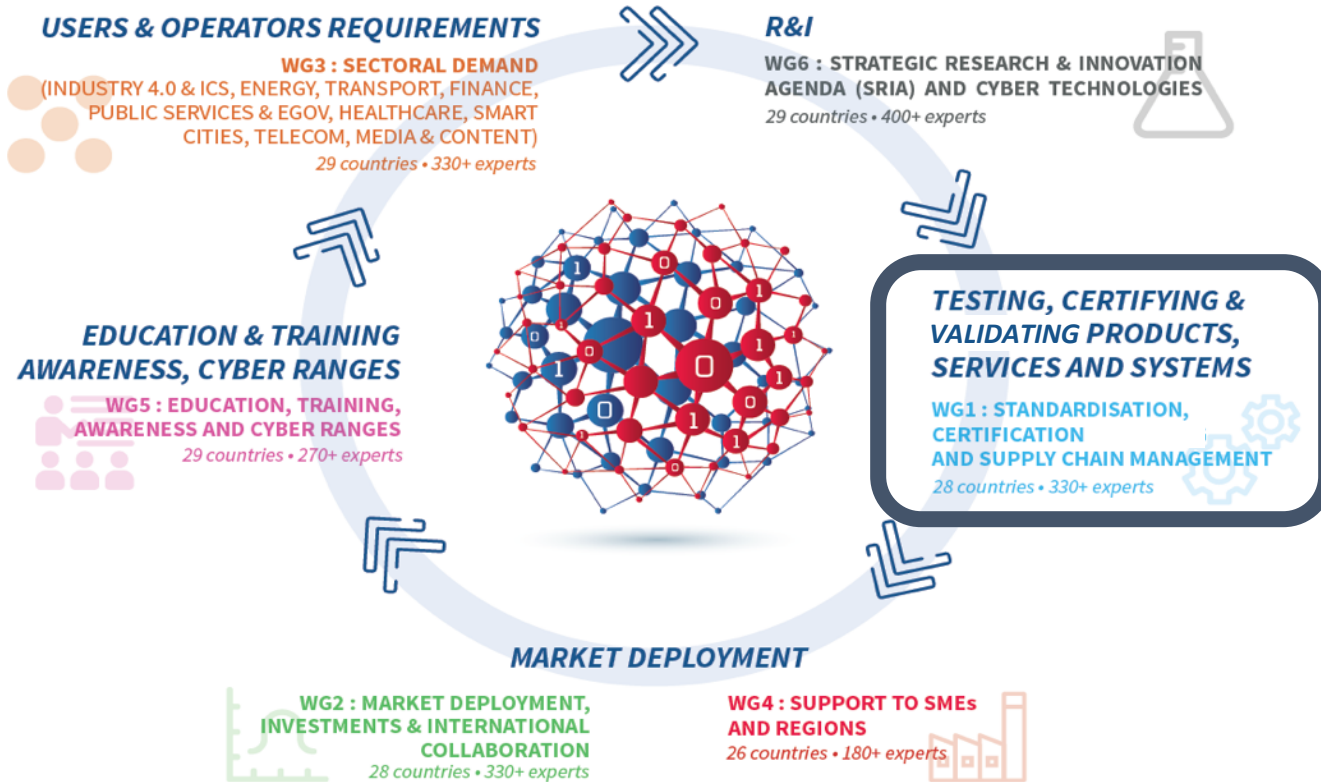# Trustworthy and cyber resilient Digital Europe

Roberto Cascella

ECSO Secretariat

Cyberwatching.eu webinar: Cybersecurity risk management
– Online, 23 November 2020 –

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

USERS & OPERATORS REQUIREMENTS

WG3 : SECTORAL DEMAND
(INDUSTRY 4.0 & ICS, ENERGY, TRANSPORT, FINANCE, PUBLIC SERVICES & EGOV, HEALTHCARE, SMART CITIES, TELECOM, MEDIA & CONTENT)
29 countries • 330+ experts

R&I

WG6 : STRATEGIC RESEARCH & INNOVATION AGENDA (SRIA) AND CYBER TECHNOLOGIES
29 countries • 400+ experts

Reminder

EDUCATION & TRAINING AWARENESS, CYBER RANGES

WG5 : EDUCATION, TRAINING, AWARENESS AND CYBER RANGES
29 countries • 270+ experts

TESTING, CERTIFYING & VALIDATING PRODUCTS, SERVICES AND SYSTEMS

WG1 : STANDARDISATION, CERTIFICATION AND SUPPLY CHAIN MANAGEMENT
28 countries • 330+ experts

MARKET DEPLOYMENT

WG2 : MARKET DEPLOYMENT, INVESTMENTS & INTERNATIONAL COLLABORATION
28 countries • 330+ experts

WG4 : SUPPORT TO SMEs AND REGIONS
26 countries • 180+ experts

ECSO coordinates its cybersecurity activities in Europe (R&I and market issues) with the different main EU actors

Reminder

EU Initiatives - PPPs, JUs

European Institutions

European sectoral associations

European Agencies

National Public Bodies

Non-EU Public administrations

International Bodies

WG1 – Standardisation, Certification, and Supply Chain Management
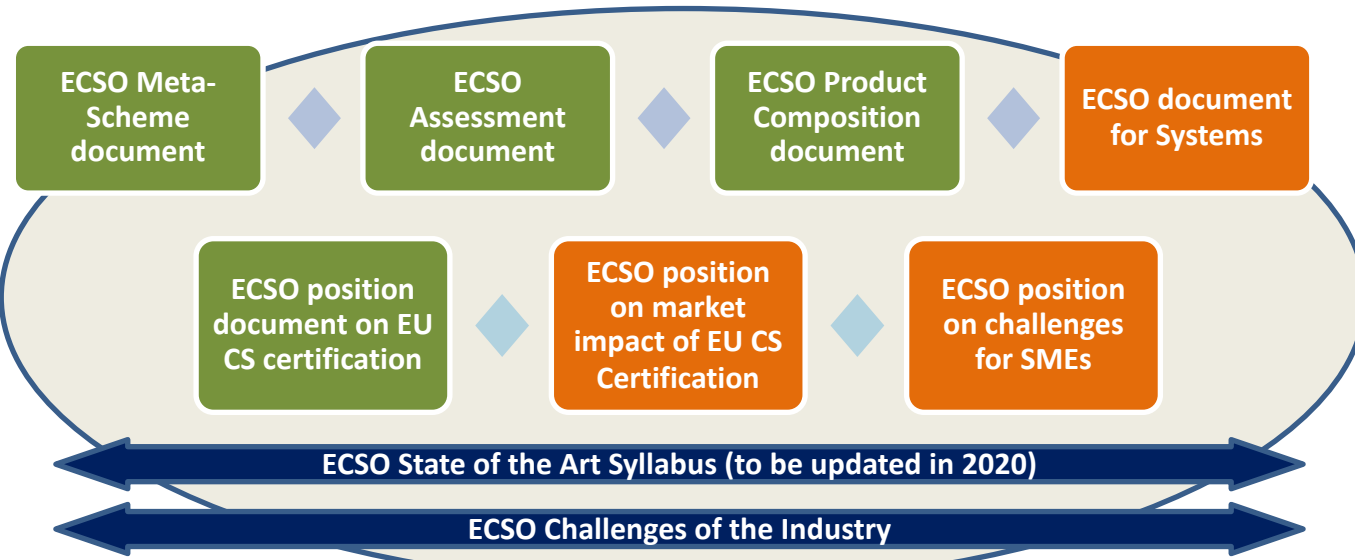
Connected Components

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

ECS — EUROPEAN CYBER SECURITY ORGANISATION

ECSO Meta-Scheme document	**ECSO Assessment document**	**ECSO Product Composition document**	**ECSO document for Systems**

ECSO position document on EU CS certification	**ECSO position on market impact of EU CS Certification**	**ECSO position on challenges for SMEs**

ECSO State of the Art Syllabus (to be updated in 2020)

ECSO Challenges of the Industry

Additional activities 2020-2021

➢ Support to Policy implementation: Contribution to ECSO WG6 on DEP priorities describing challenges and plan for the future. Development of capabilities for certification and assessment.

➢ Consider the consistency of the legislative framework and Cybersecurity Act

Collaborations

ECSO member of SCCG

Advise EC and ENISA on strategic issues regarding cybersecurity certification, and assist EC in the preparation of the Union's rolling work programme

MoU with CEN CENELEC & ETSI

• Contribute to **Standard on MSSP**
• Contribute to the **Cybersecurity lightweight evaluation methodology for ICT products**

Work with EC and ENISA

• MSP & **ICT Standardisation Rolling Plan**
• JRC on **Industrial and Automated Control System**

ECSO Product Certification Composition

- **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
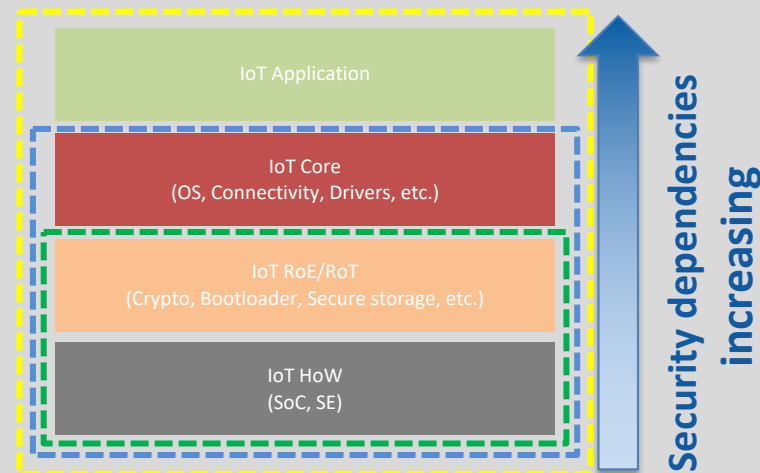
ECS

European Cyber Security Certification
Product Certification Composition
WG1 – Standardisation, certification and supply chain management
November 2020

www.ecs-org.eu

ECSO Product Certification Composition

Composition document – underlying principles and practical aspects

- Initial considerations for composition:
  - <u>Bottom-up, top-down, mix</u>
  - 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**

IoT Application

IoT Core
(OS, Connectivity, Drivers, etc.)

IoT RoE/RoT
(Crypto, Bootloader, Secure storage, etc.)

IoT HoW
(SoC, SE)

Security dependencies increasing

ECSO position document on EU CS certification

European Cyber Security Certification
Challenges ahead for the roll-out of the Cybersecurity Act
WG1 – Standardisation, certification and supply chain management
November 2020

- Understand the main challenges that could hinder the usage of future European cybersecurity certification schemes across industries

- The goal is to identify the necessary future steps and aspects that ECSO WG1 should investigate in the coming months

www.ecs-org.eu

1. Cybersecurity Framework Consistency

2. Composition of evidence and considerations for system integrators

3. Analysis of priorities for cybersecurity certification based on market needs

Market impact and SMEs challenges

- The value of certification for the market and potential gaps

- Importance of the supply chain in the era of digital transformation

- Sovereignty & business continuity of global supply chains

- Complexity and difficulties for SMEs of the current options for certification

- Vulnerability and risk management

- Challenges for a consistence mapping between risk and assurance levels

- Importance of a time and cost-effective certification process

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