ECSO activities in support of the EU Cybersecurity Act

Roberto Cascella
ECSO Secretariat

Shaping the future of cybersecurity
Priorities, challenges and funding opportunities for a more resilient Europe
– Online, 13 July 2021 –

Vision

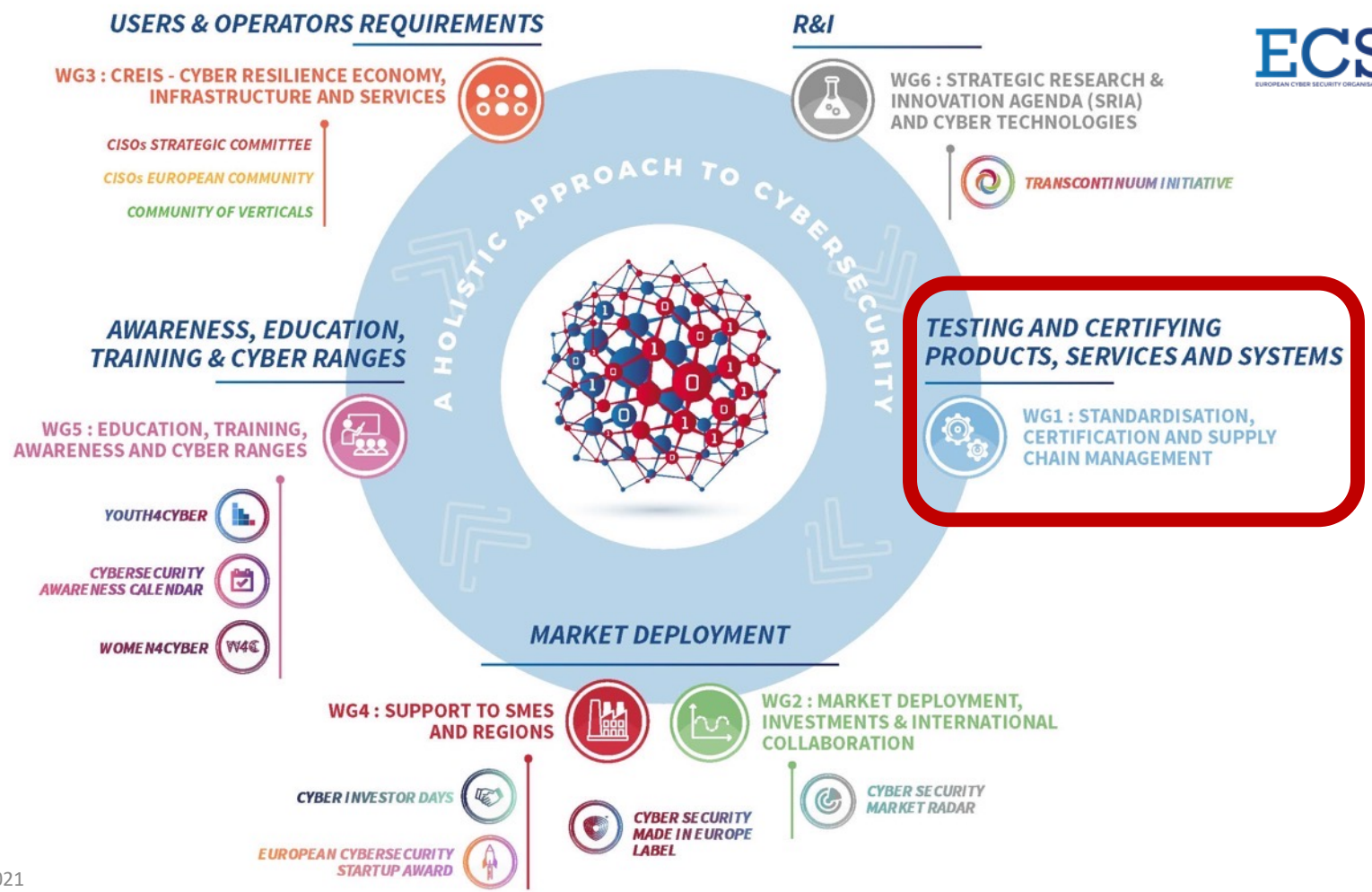
ECSO endeavours to support the achievement of a Cyber resilient digital Europe and increase European Digital Sovereignty & Strategic Autonomy through the establishment of trusted & resilient supply chains for cybersecurity solutions and services.

To achieve this Vision, ECSO implements its Strategy and drives its Actions at short, medium and long term also considering political, economic, societal context and technology drivers.

Cyber Resilient Digital Europe

-

European Digital Sovereignty & Strategic Autonomy


USERS & OPERATORS REQUIREMENTS
WG3 : CREIS - CYBER RESILIENCE ECONOMY, INFRASTRUCTURE AND SERVICES
CISOs STRATEGIC COMMITTEE
CISOs EUROPEAN COMMUNITY
COMMUNITY OF VERTICALS
R&I
WG6 : STRATEGIC RESEARCH & INNOVATION AGENDA (SRIA) AND CYBER TECHNOLOGIES
TRANSCONTINUUM INITIATIVE
A HOLISTIC APPROACH TO CYBERSECURITY
AWARENESS, EDUCATION, TRAINING & CYBER RANGES
WG5 : EDUCATION, TRAINING, AWARENESS AND CYBER RANGES
YOUTH4CYBER
CYBERSECURITY AWARENESS CALENDAR
WOMEN4CYBER
TESTING AND CERTIFYING PRODUCTS, SERVICES AND SYSTEMS
WG1 : STANDARDISATION, CERTIFICATION AND SUPPLY CHAIN MANAGEMENT
MARKET DEPLOYMENT
WG4 : SUPPORT TO SMES AND REGIONS
CYBER INVESTOR DAYS
EUROPEAN CYBERSECURITY STARTUP AWARD
CYBER SECURITY MADE IN EUROPE LABEL
WG2 : MARKET DEPLOYMENT, INVESTMENTS & INTERNATIONAL COLLABORATION
CYBER SECURITY MARKET RADAR

WG1 - Standardisation, certification & supply chain management

Working Group 1 (WG1) is composed of certifiers, test labs, component manufacturers, system integrators, service providers, national public administrations, RTOs, etc.

The objective of this WG is to support the roll-out of EU ICT security certification schemes, standard and legislative recommendations, and ensure the establishment of trusted and resilient supply chains in Europe.
The activities of WG1 is structured around 2 main pillars:

Define methodologies and approaches. Provide guidelines & recommendations on European legislations and policy initiatives.

Cooperation with ESOs, EU Institutions (European Commission, ENISA, MSP) and other bodies (CEN/CENELEC, ETSI, etc).

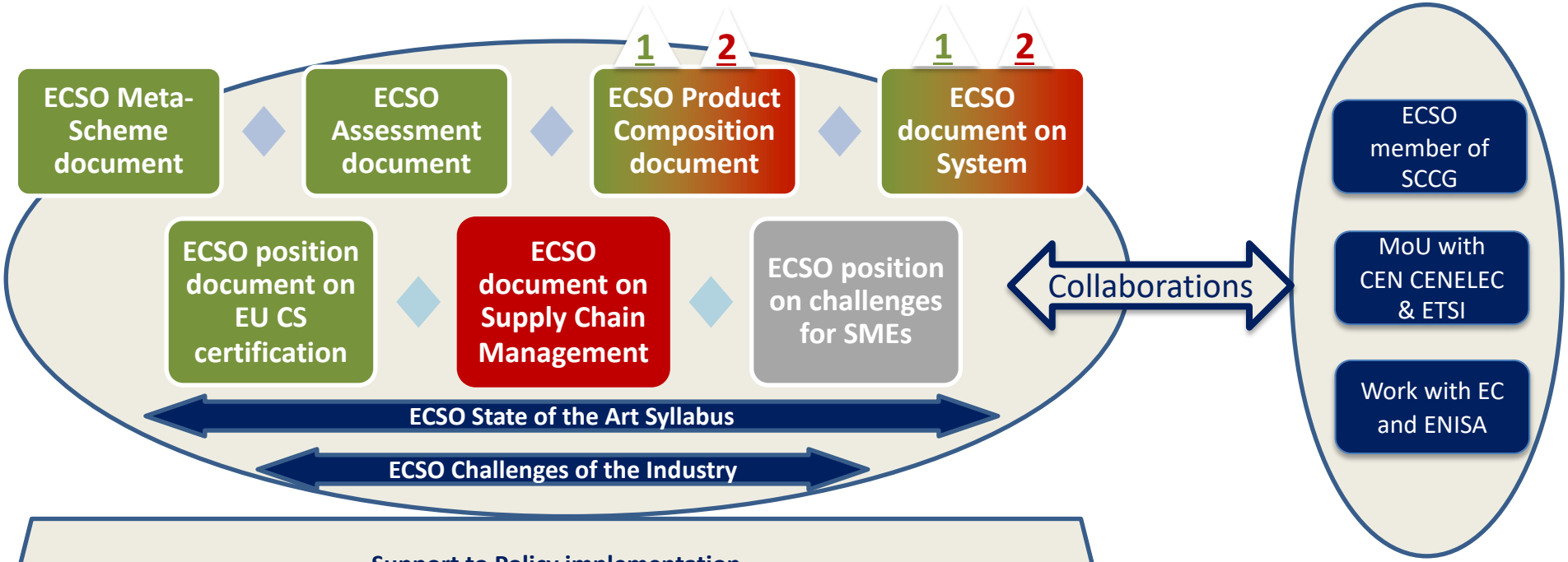
SWG 1.1 – Connected Components
Work on the inter-relationship (“composition”) of EU scheme certified components based on standards for trusted supply chain and product certification in line with to the EU Cyber Act.

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 & supply chain management

New work items



Support to Policy implementation

Consistency of the legislative framework and Cybersecurity Act (cooperation with ECSO Legal and Regulation Task Force)

ECSO position document on EU CS certification

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

- Understand the main challenges that could hinder the usage of future European cybersecurity certification schemes across industries
- Aspects considered
    1. Cybersecurity Framework Consistency
    2. Composition of evidence and considerations for system integrators
    3. Analysis of priorities for cybersecurity certification based on market needs

Cybersecurity Framework Consistency

- Consistency is key to setting trustable and reliable certification schemes that are recognised and used by all stakeholders and a cost effective certification process for any applicant
- Some of the challenges ahead
  - Mapping of security assurance levels and the risk
  - Diversity of applications, products, systems and services
  - Diversity of market sectors and their stakeholders
  - …
- Pillars to ensure framework consistency
  - Consistent definition of the Security Level of Assurance and risk based approach for mapping
  - Promotion and enhancement of international and/or recognised standards
  - Common or similar methods and methodologies of assessment and testing
  - Harmonised approaches and processes of CABs and testing labs through a governance and a market surveillance
  - …

Analysis of priorities for cybersecurity certification based on market needs

- Encourage, define, monitor, assess and help companies improving the overall security of their products
  - Automated tools for certification simplification and speeding up the whole process
- Identify the family of security or non-security products EU has strategically intention to develop further and became global reference in terms of reliability and resilience
- Promote efficiency and cost effectiveness, e.g. reduced amount of horizontal and vertical schemes
- Address specific technical, operational and regulatory requirements of the targeted market via vertical certification schemes
- 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

ECSO Product Certification Composition

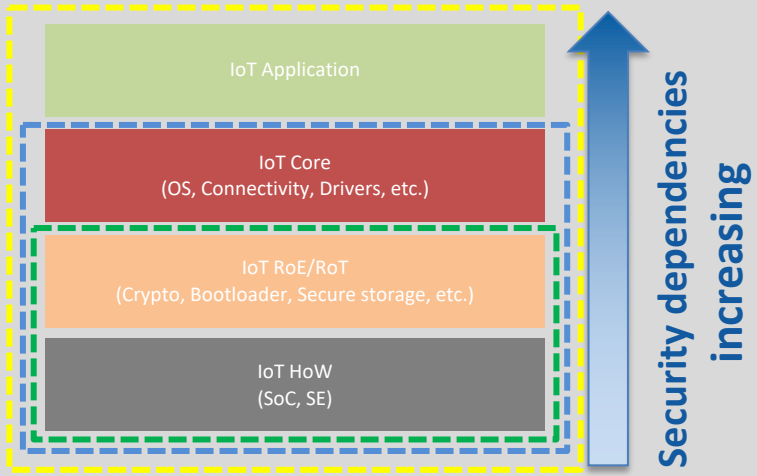
Available at https://ecs-org.eu/documents/publications/5fbfc8436e5a1.pdf

- **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

ECSO Product Certification Composition

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 - Objectives 2021

- 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 and explain system and service lifecycle and associated risk management.
- 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 policy implementation: link with DEP priorities describing challenges and plan for the future. Development of capabilities.
- Continue and strengthen collaborations with ENISA, EC, European SDOs and other relevant stakeholders.

CYBERSECURITY™
MADE IN EUROPE

WHAT IS?

CYBERSECURITY MADE IN EUROPE is an industry-driven marketing tool, designed to promote European cybersecurity companies and increase their visibility on the European and on the global market.

The lack of such marketing tool inspired European Cyber Security Organisation (ECSO) to develop the label.

WHAT ARE THE BENEFITS?

The Label serves as a market differentiator based on geographic location.

The Label raises awareness of the strategic value of cybersecurity companies originating in Europe and developing their business based on trusted European values.

The Label increases companies' visibility among potential business partners, end-users and cybersecurity investors.

ECS
EUROPEAN CYBER SECURITY ORGANISATION

European Cyber Security Organisation (ECSO)
29, Rue Ducale
1000 - Brussels
BELGIUM

secretariat@ecs-org.eu

www.ecs-org.eu

@ecso_eu

ecso-cyber-security

Join the Community

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

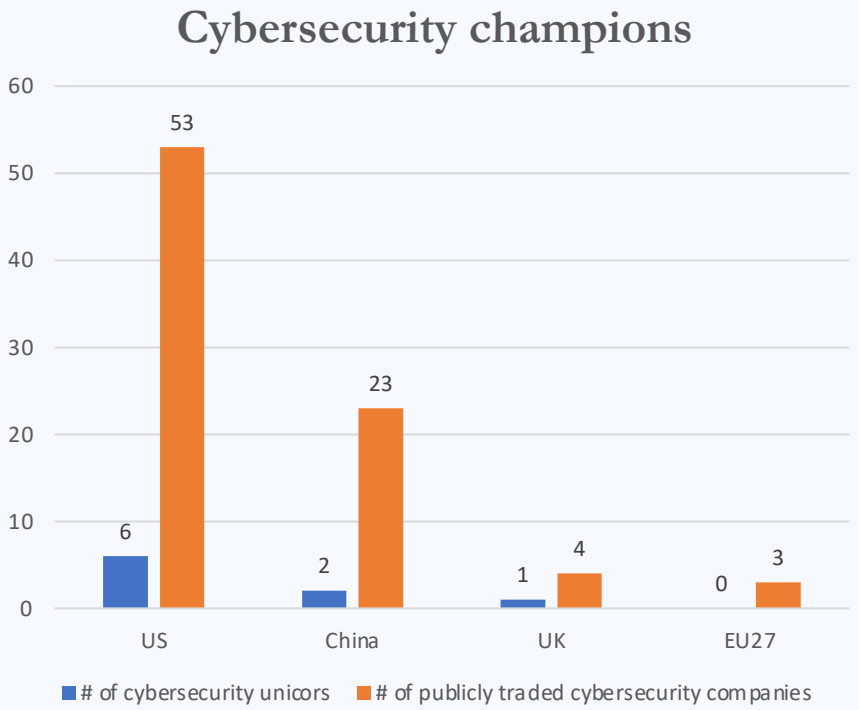
It discusses the aspects that could hinder the usage of future European cybersecurity certification schemes across industries

WHY THE LABEL?

Globally cybersecurity is one of the fastest growing strategic markets. In Europe, however, it remains highly fragmented.

74% of the European cybersecurity companies are micro companies and SMEs.

Absence of international marketing and business development initiatives focusing on supporting the growth and facilitating the competitiveness of the European cybersecurity pure players.



LABELLED COMPANIES

Since its launch in November 2021, around **25 labels have been issued** to European cybersecurity companies. Here are a few of them:

arbit

enigmedia

clavister

Banshie

SECTION

STM

R.iT

DISCOVER THE SPIR.iT OF EXCELLENCE.
SURPASS YOUR SUCCESS.

PHYSEC
SECURITY FOR THINGS

TEHTRIS
FACE THE UNPREDICTABLE

DENCRYPT

ZYBERSAFE

KOSEC

Around **20 applications are under the verification process.**

WHAT IS NOT?

The Label is not a certification tool.

The Label issuance process does not require a technical audit, but relies on self-declaration.

The Label does not target specific cybersecurity products or services, but European-based cybersecurity companies.

The Label focuses on European cybersecurity startups and SMEs, but does not exclude large companies.

The Label does not compete with similar national labels and can be used in conjunction with them.

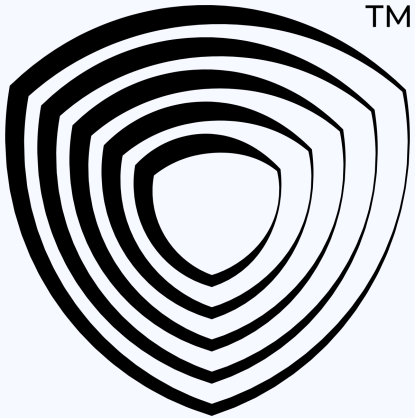
HOW LONG IS IT VALID?

The Label is valid for the period of 12 months.

If the company wants to continue carrying the Label after the validity expires, it commits to indicate all the relevant changes which have taken place since the last eligibility check and approval. In case of no relevant changes, the re-issuance takes place automatically once the payment is received.

WHO CAN APPLY?

The Label is granted to European cybersecurity companies from the European Union (EU27), European Free Trade Association (EFTA) and European Economic Area (EEA) countries, as well as from the United Kingdom (UK).



WHAT ARE THE CRITERIA?

In order to qualify for the Label, prospective cybersecurity companies will be required to prove that:

1. They are headquartered in Europe.
2. They have no major ownership/control from outside of Europe.
3. Europe is their primary business place with more than a half of their cybersecurity R&D activities and staff located there.
4. They provide trustworthy cybersecurity solutions, as defined in ENISA's 'Indispensable baseline security requirements for the secure ICT products and services'.
5. They respect European data and privacy requirements, defined by the EU's General Data Protection Regulation (GDPR).

HOW MUCH DOES IT COST?

Each qualified issuing association has discretionary power to decide the pricing of the Label, depending on the administrative costs it experiences and the membership benefits it offers to its members.

We invite companies to contact the qualified issuing partners of your choice for detailed information about the pricing.

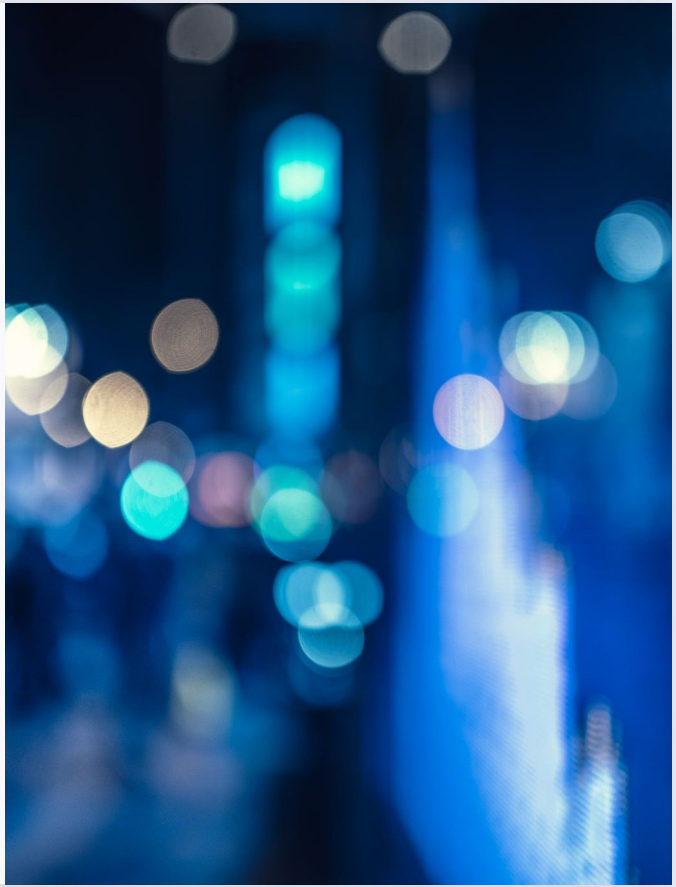
CYBERSECURITY™
MADE IN EUROPE

WHO ISSUES THE LABEL?

Only qualified issuers authorised by the European Cyber Security Organisation (ECSO) has the right to issue the Label. Their contacts are available on the ECSO website and below in this presentation.

Prospective companies can choose any qualified issuer of their choice regardless of the country in which their European headquarters are located.

ECSO does not accept applications from companies and does not issue the Label. However, it remains the sole owner and supervisor of the Label scheme.



16 qualified issuing partners from all over Europe