ECS

EUROPEAN CYBER SECURITY ORGANISATION

Benefits of Product Certification Composition

Roberto Cascella

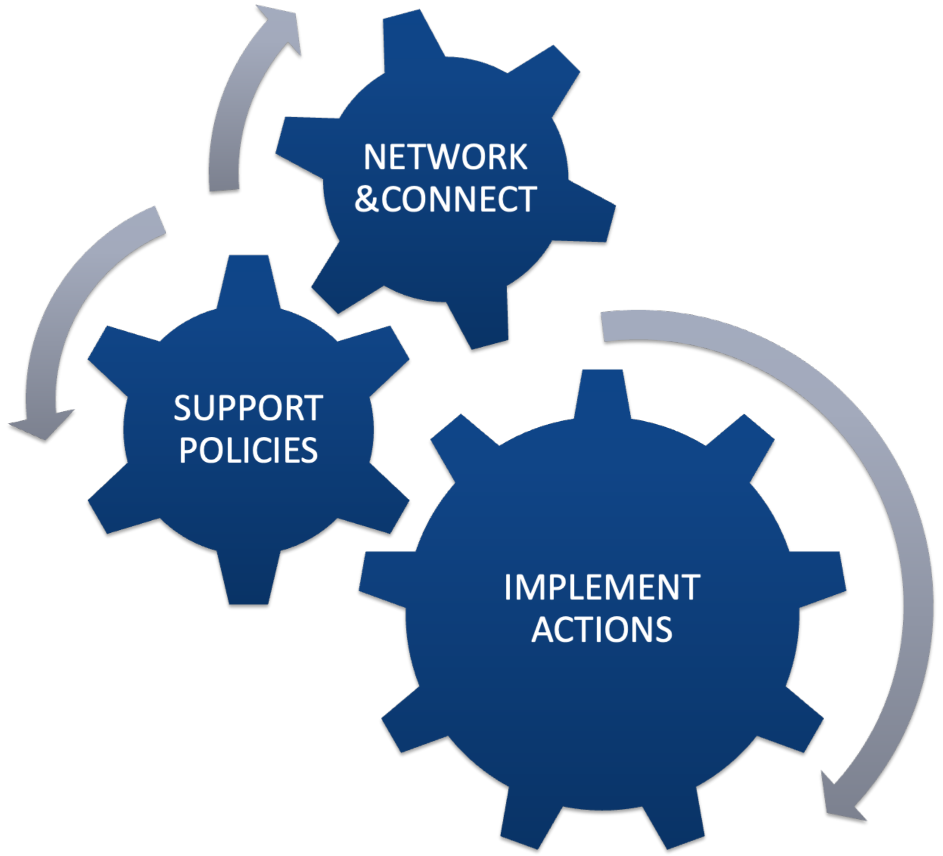
SESIP - Simplifying Security Evaluation in IoT

19 October 2022

ECSO Mission & Approach

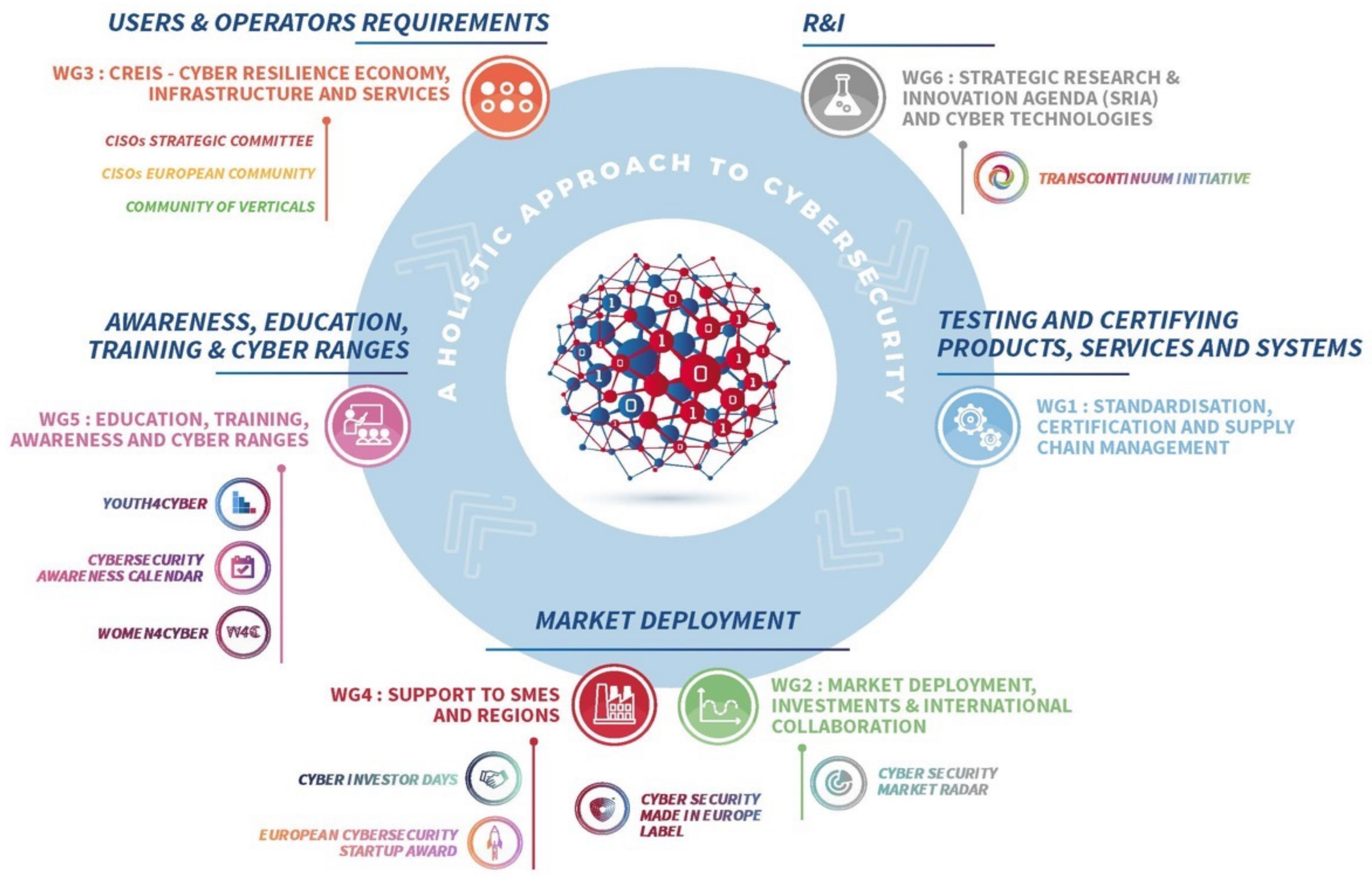
WHAT?

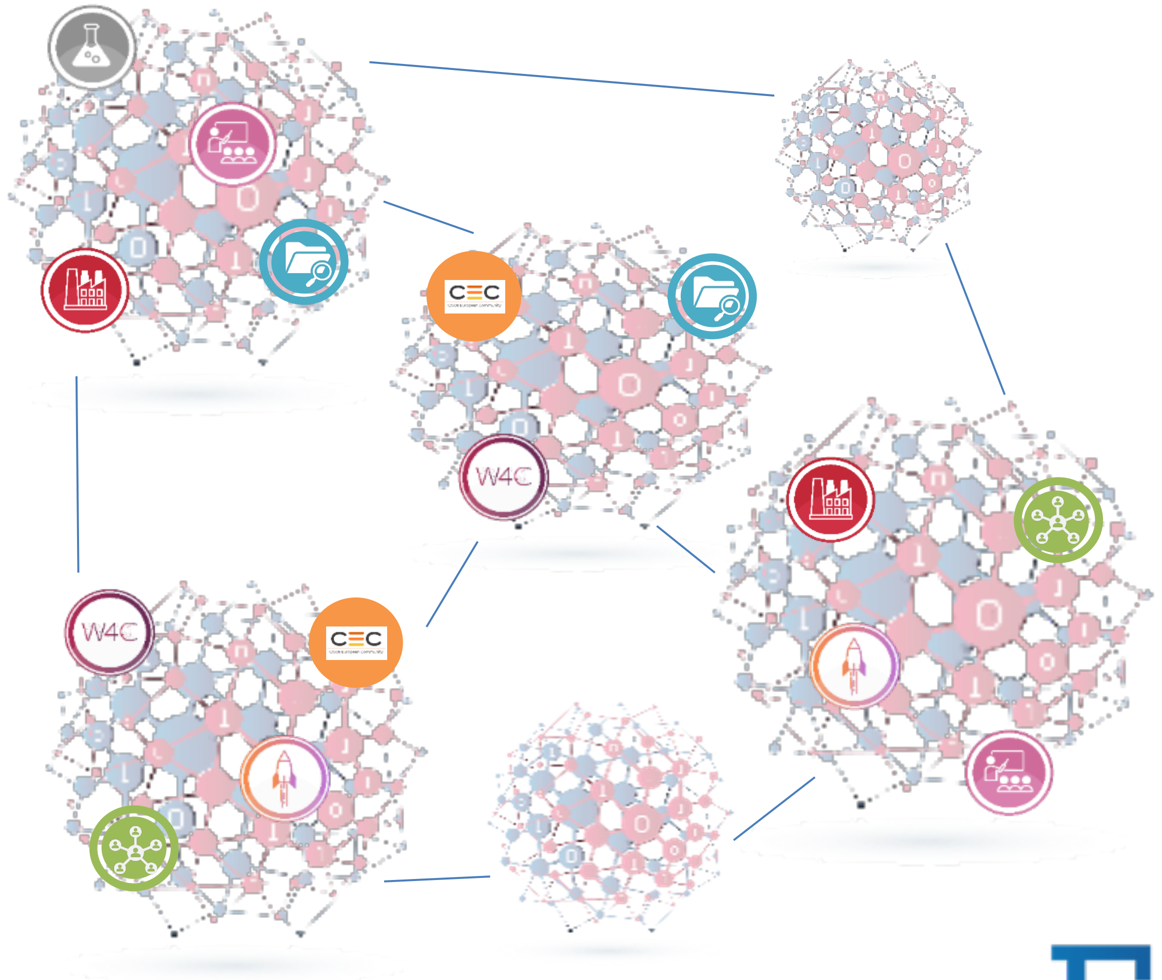
- ECSO contributes to the **European Digital Sovereignty & Strategic Autonomy** and to the strenghtening of **Europe's cyber resilience**



HOW?

- By empowering communities and shaping the European cybersecurity ecosystem
- By federating and providing a platform for collaboration for various stakeholders
- By bringing together the private and public sectors, facilitating their dialog and joint actions


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
W4C
TESTING AND CERTIFYING PRODUCTS, SERVICES AND SYSTEMS
WG1 : STANDARDISATION, CERTIFICATION AND SUPPLY CHAIN MANAGEMENT
MARKET DEPLOYMENT
WG4 : SUPPORT TO SMES AND REGIONS
WG2 : MARKET DEPLOYMENT, INVESTMENTS & INTERNATIONAL COLLABORATION
CYBER INVESTOR DAYS
EUROPEAN CYBERSECURITY STARTUP AWARD
CYBER SECURITY MADE IN EUROPE LABEL
CYBER SECURITY MARKET RADAR



Communities → **Ecosystems**

ECS
EUROPEAN CYBER SECURITY ORGANISATION

Overview of ECSO Members

Large companies (users and providers)

SMEs & start-ups

Research centres, Universities

European, National and Regional clusters & associations

Local, regional and national public administrations

Investors

End-users and operators of critical infrastructures and essential services

As of today, ECSO counts 273 Members

WG1 - Standardisation, Certification and Supply Chain Management

Our activities

Support the roll-out of EU ICT security certification schemes, standard and legislative recommendations by:

- Understanding and presenting the industry’s challenges when using standards and certification schemes
- Understanding the needs of the market, identifing the gaps in standardisation and proposing a roadmap for priorities
- Defining methodologies and approaches to facilitate and support the use of certification schemes

Facilitate the establishment of trusted and resilient supply chains in Europe by:

- Analysing the impact of cybersecurity policies and regulations on the market from a technical perspective, and providing guidelines & recommendations on legislations and policy initiatives
- Analysing and defining best practices for organisations, both product / service providers and users / integrators

Who participates?

Certifiers, test labs, component manufacturers, system integrators, service providers, national public administrations and RTOs.

Collaborations

ETSI CEN CENELEC

enisa

European Commission

Stakeholder Cybersecurity Certification Group

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
  - ➢ 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

Customers: Certification provides the appropriate level of confidence that specific requirements have been fulfilled.

Vendors: Certification demonstrates that their products or services have been attested to fulfill specific requirements.

CABs: Conformity assessment bodies provide independent evaluation on products' compliance and issue certificates that attest the objective unbiased verification of the certified product.

Challenges of the industry: some examples

Vendors

Maintaining compliance is tough. Components in the product are not all certified using the same schemes or at the same assurance levels.

Monitoring suppliers' activities to meet a product's multi-certification requirements is not easy.

Many schemes are not cheap and have overlapping requirements with other schemes

CABs

Achieving, maintaining and renewing accreditation for different schemes is time consuming and resource inefficient.

While the scope of some schemes is too narrow and thus unusable in multiple domains, others are too generic in scope, complicated and expensive to implement.

Many schemes are not cheap and have overlapping requirements with other schemes.

Our documents

Product Certification Composition
Supply chain management
System Security and Certification Considerations

Product Certification Composition

Achieve cost effective certification using different schemes (products, processes and services)

- Scheme composition is a key factor allowing to build a trusted and resilient multi-technological domains using horizontal components to build an end-product

System Security and Certification Considerations

Systems are mission specific, and the risk is managed for its full dimension crossing all life cycle stages from design, procurement, testing, integration, implementation, operation, maintenance, retrofit and decommissioning.

- Relevance of the cyber security risk perimeter and of a high-level risk assessment done in a coherent framework
- Important security notions of the system lifecycle: governance, maturity and diversity of processes, products and people that can design, build and ultimately run a mission-specific system

Supply chain management

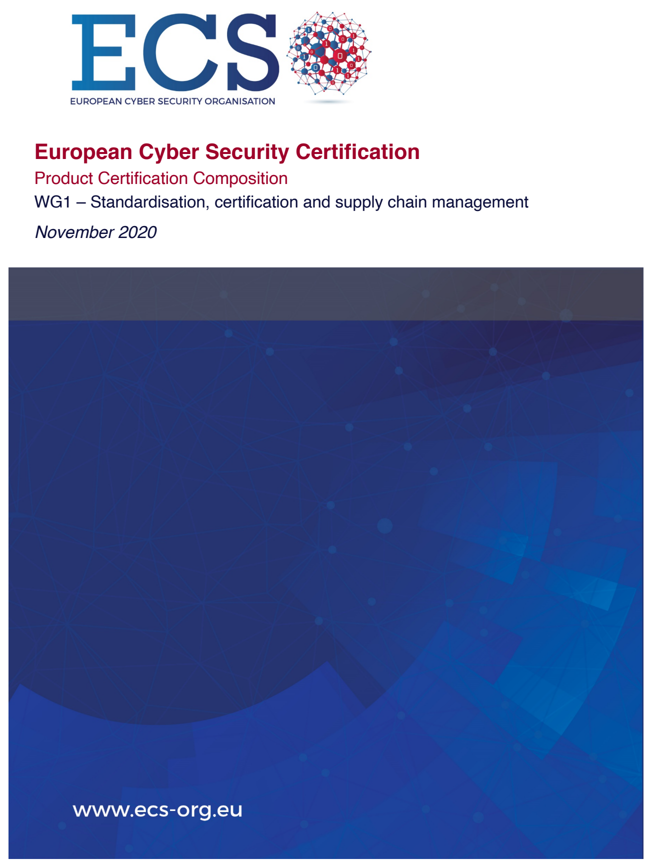
Assess the integrated products and focus on best practices to ensure that the suppliers are trustworthy and demonstrate in a harmonized way the capabilities and the security of the products / services / systems

- Relevance for policy aspects: NIS2, Cyber Resilience Act, …

ECSO Product Certification Composition

Goal: Support a Supply Chain of Trust - knowing from where you're sourcing components, software or hardware and trusting the security inside while having full visibility of each layer of security through 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 ORGANISATION

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

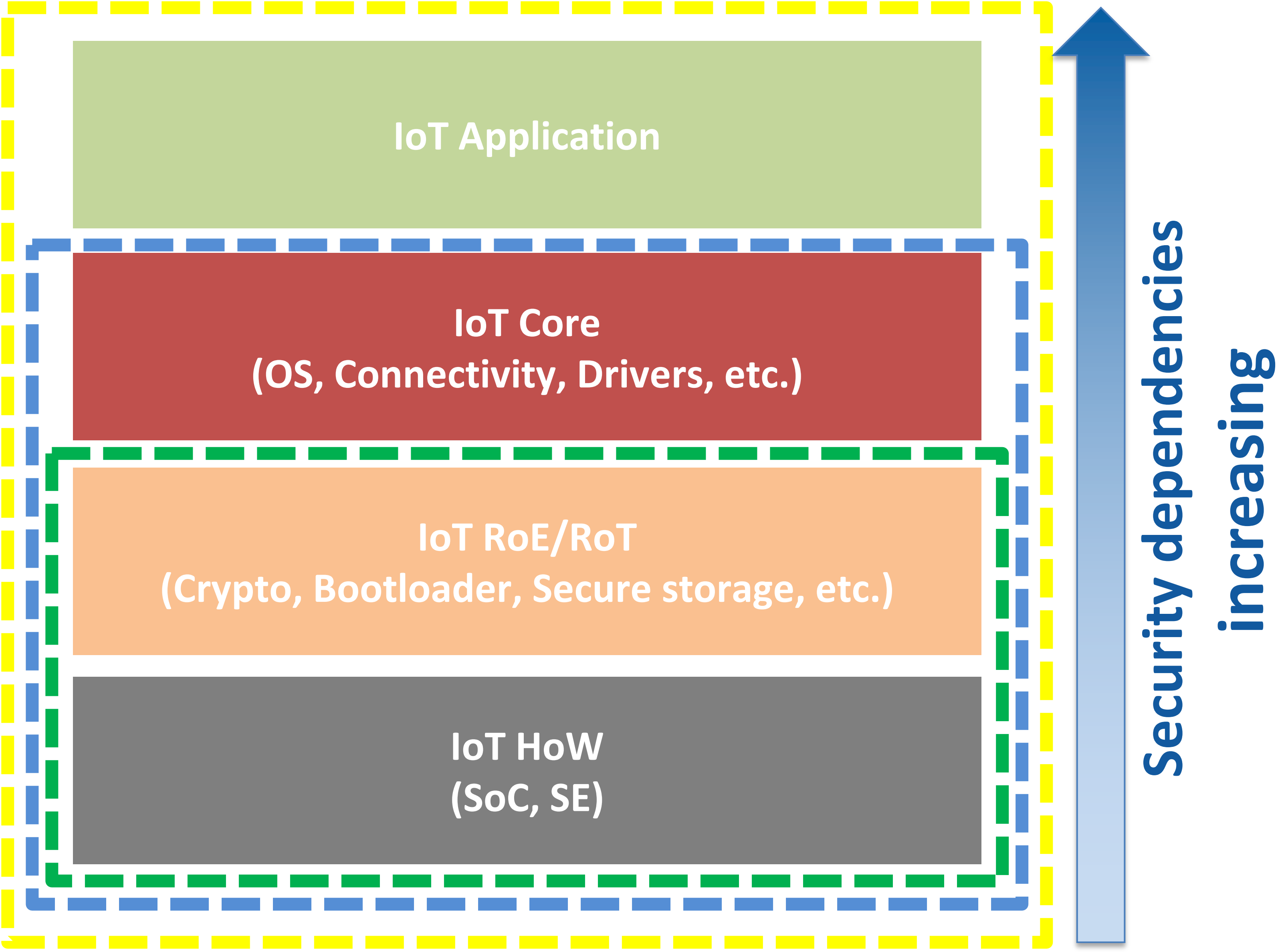
www.ecs-org.eu

Available at https://ecs-org.eu/publications?f=11

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**


IoT Application
IoT Core
(OS, Connectivity, Drivers, etc.)
IoT RoE/RoT
(Crypto, Bootloader, Secure storage, etc.)
IoT HoW
(SoC, SE)
Security dependencies increasing

ECSO Product Certification Composition

Challenges for an effective schemes' composition

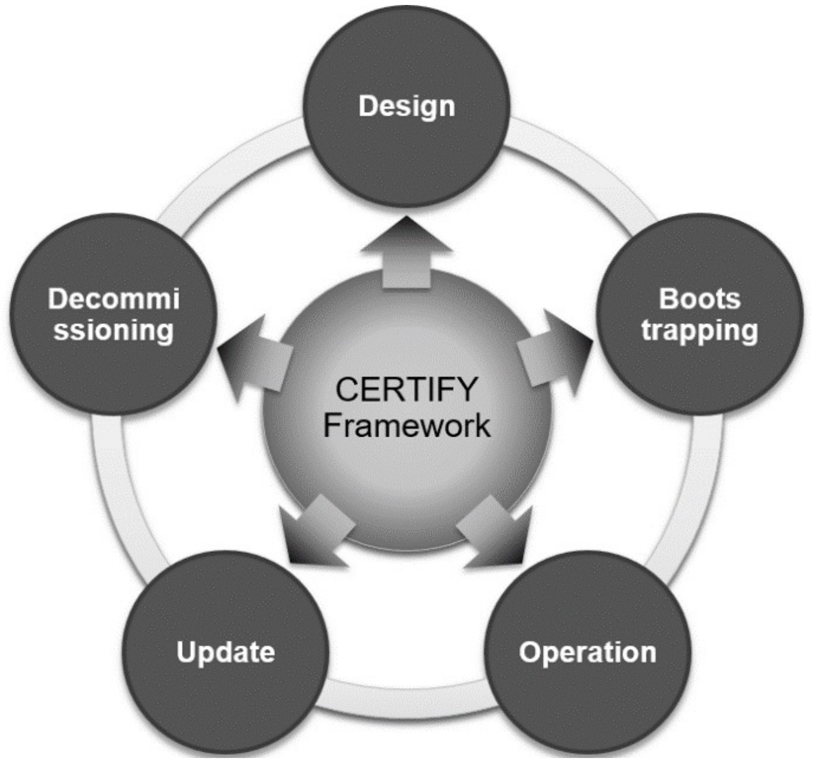
- Harmonized notion of “intended use”
- Risk assessment approach
- Comparable assurance levels, e.g., a substantial level should be comparable from one scheme to another, e.g., in term of effort from the CAB and obligations on the product provider
- Output Information from a certification (beyond the certificate)
  - e.g., CC/EUCC security target need a CC expert reader but some information such as security assumption about the deployment environment are crucial for the integrator

aCtive sEcurity foR connecTed devIces liFecYcles (10/22 – 09/25)

CERTIFY

CERTIFY defines a methodological, technological, and organizational approach towards IoT security lifecycle management based on

i. security by design support,
ii. continuous security assessment and monitoring
iii. timely detection, mitigation, and reconfiguration,
iv. secure IoT Over-The-Air (OTA) updating, and
v. continuous security information sharing.



- CERTIFY will validate the architecture through cutting-edge use-cases and pave the way towards innovative security in a broad spectrum of IoT environments
- CERTIFY will develop a dynamic runtime security evaluation methodology to verify lifecycle-wide IoT device security and continuous (re-)certification methodology

Composition within the same scheme or across scheme can facilitate the (re-)certification following a change in security requirements and threat landscape

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 101069471 .
This material reflects only the authors' view and European Commission is not responsible for any use that may be made of the information it contains.

Key takeaways

Build a trusted and resilient multi technological domains using horizontal components to build an end-product

Cost effective certification using different schemes (products, processes and services)

Composition is considered as a certification enabler because it facilitates using multiple components by multiple suppliers

ECSO

EUROPEAN CYBER SECURITY ORGANISATION

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

secretariat@ecs-org.eu

www.ecs-org.eu

@ecso

Benefits of becoming a Member of ECSO

JOIN ECSO's policy Task Force and Working Groups

BOOST your market visibility

GAIN ACCESS to investments and funding opportunities at EU and national levels

TAKE THE LEAD in proposing new initiatives and services to build the European cybersecurity Market

GROW your business network with other members of the Community

SHARE information and best practices with your counterparts

INTERACT with legislators and decision makers at EU and national level

BE PART OF the organisation federating the European cybersecurity community

RECEIVE TIME-SENSITIVE POLICY UPDATES straight into your inbox

GET INVOLVED in ECSO's six Working Groups (WG), task forces and in over ten initiatives of choice

GAIN THE OPPORTUNITY to manage the organisation and drive common opinions

VISIBILITY though ECSO channels, targeting European cybersecurity stakeholders

COMMUNICATION activities to promote your content via articles, interviews, blogs and more, published on a dedicated Member section and shared on ECSO's newsletter

UNLIMITED ACCESS to the ECSO Cybersecurity Awareness Calendar