ECSO
EUROPEAN CYBER SECURITY ORGANISATION

Challenges of cybersecurity certification and supply chain management

Roberto Cascella
Senior Policy Manager (ECSO Secretariat)

ECSO – EUNITY Workshop
– 24 January 2019 – Brussels

WG1 – Standardisation, certification, labelling & supply chain management

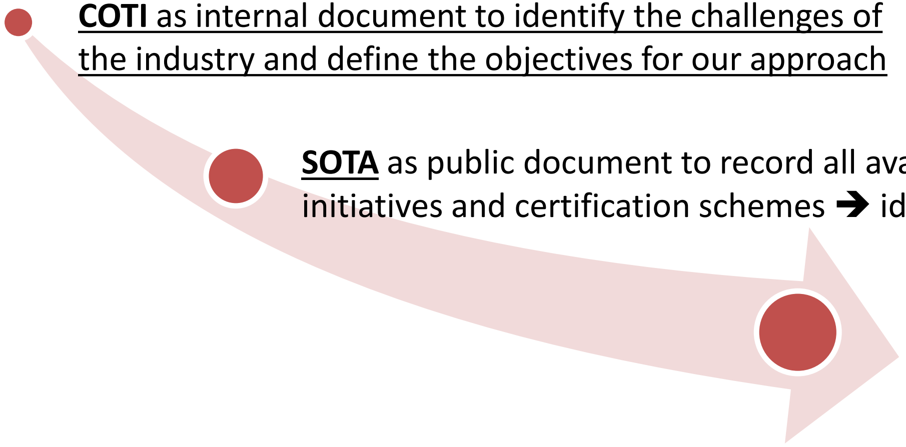
Current WG1 activities largely focus on **an updated version of the ECSO Meta-scheme approach -** how it works in practice.

Organisation of WG1

- SWG 1.1 “Self-assessment”
- SWG 1.2 “Third party assessment”
- SWG 1.3 “Base Layer”

http://www.ecs-org.eu/documents/uploads/updated-sota.pdf

http://www.ecs-org.eu/documents/uploads/european-cyber-security-certification-a-meta-scheme-approach.pdf



COTI as internal document to identify the challenges of the industry and define the objectives for our approach

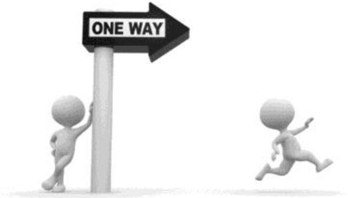
SOTA as public document to record all available cyber security standards, initiatives and certification schemes ➔ identification of existing landscape

META-SCHEME APPROACH to harmonise the minimum security required, define a unified levelling across verticals (for comparison of items), and a common way to define the scope & required security claim ➔ Foster trust by defining transparent rules

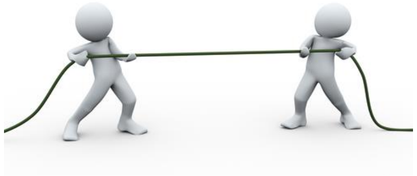
What industry worries about (examples)

EUROPEAN CYBER SECURITY ORGANISATION

Too slow and too unpredictable

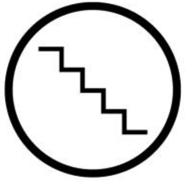


Not flexible enough



Lack of harmonization

Too much formalisms



lack of agility

Undetected cheaters in the supply chain

Static certificates

Pure checklist evaluations

complex composite certifications

*Challenges of the Industry document of ECSO WG1

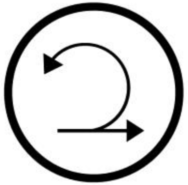
What industry expects (examples)

Fast and predictable

High level of flexibility

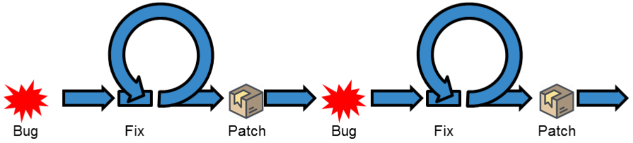
Full harmonization

Pragmatism



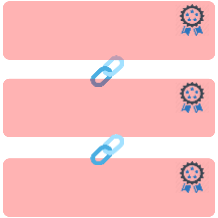
agility

Detecting cheaters
in the supply chain



Patching and updates

Ethical hacking



Lean modular composite
certifications

First of all: collection of what exists!

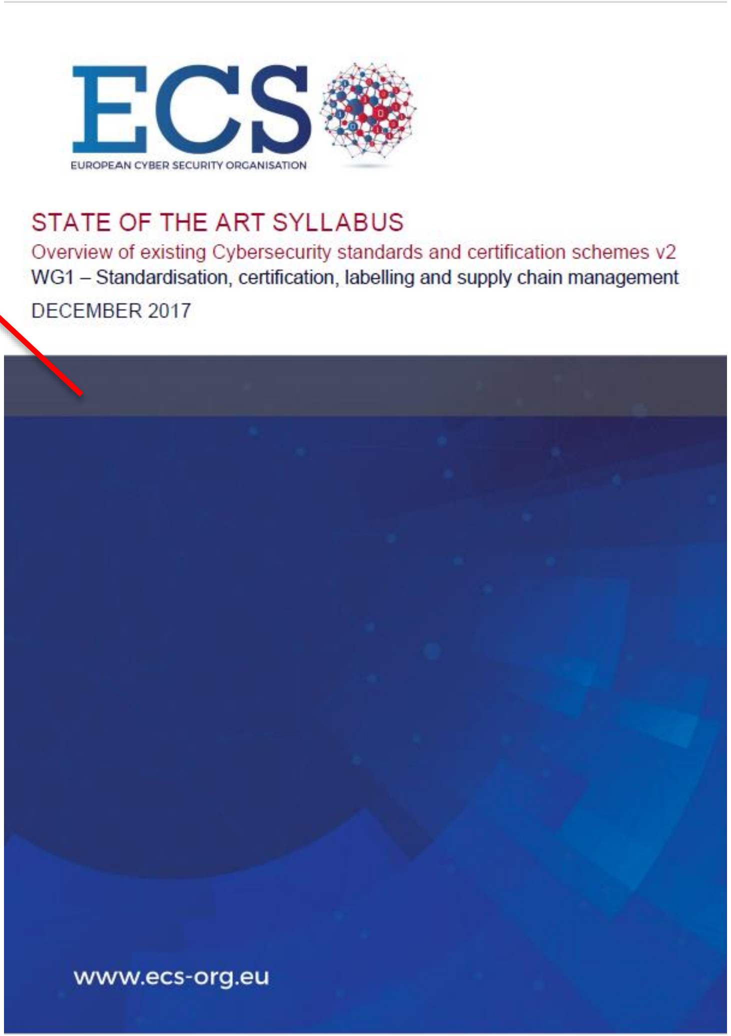
290 standards & schemes

Products & components → SOTA Chapter 3

ICT services → SOTA Chapter 4

Service providers & organisations → SOTA Chapter 5

Security professionals → SOTA Chapter 6



ECS

EUROPEAN CYBER SECURITY ORGANISATION

STATE OF THE ART SYLLABUS

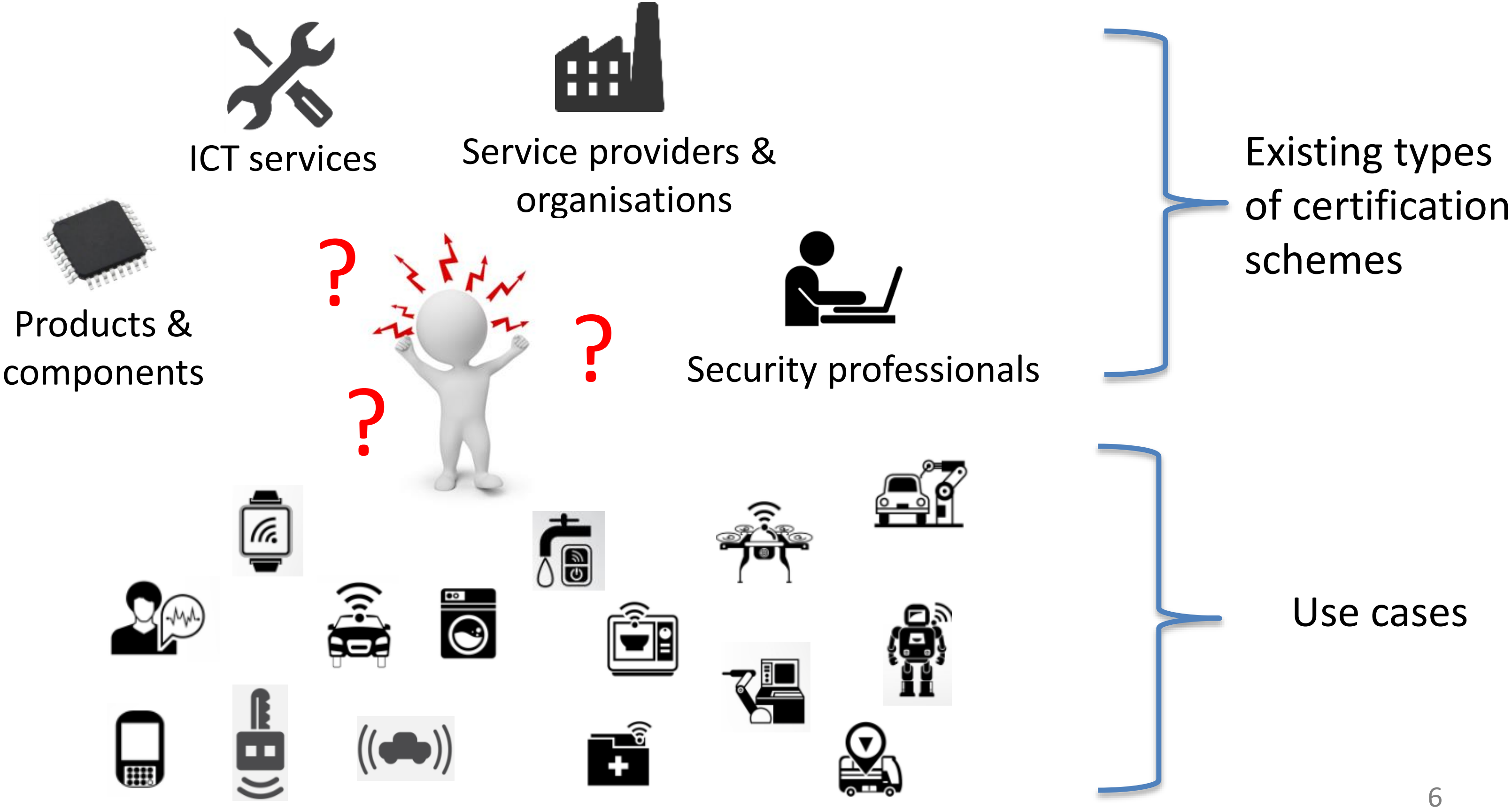
Overview of existing Cybersecurity standards and certification schemes v2

WG1 – Standardisation, certification, labelling and supply chain management

DECEMBER 2017

www.ecs-org.eu

What to do?
There is not a single scheme fitting all needs!



ICT services

Service providers & organisations

Products & components

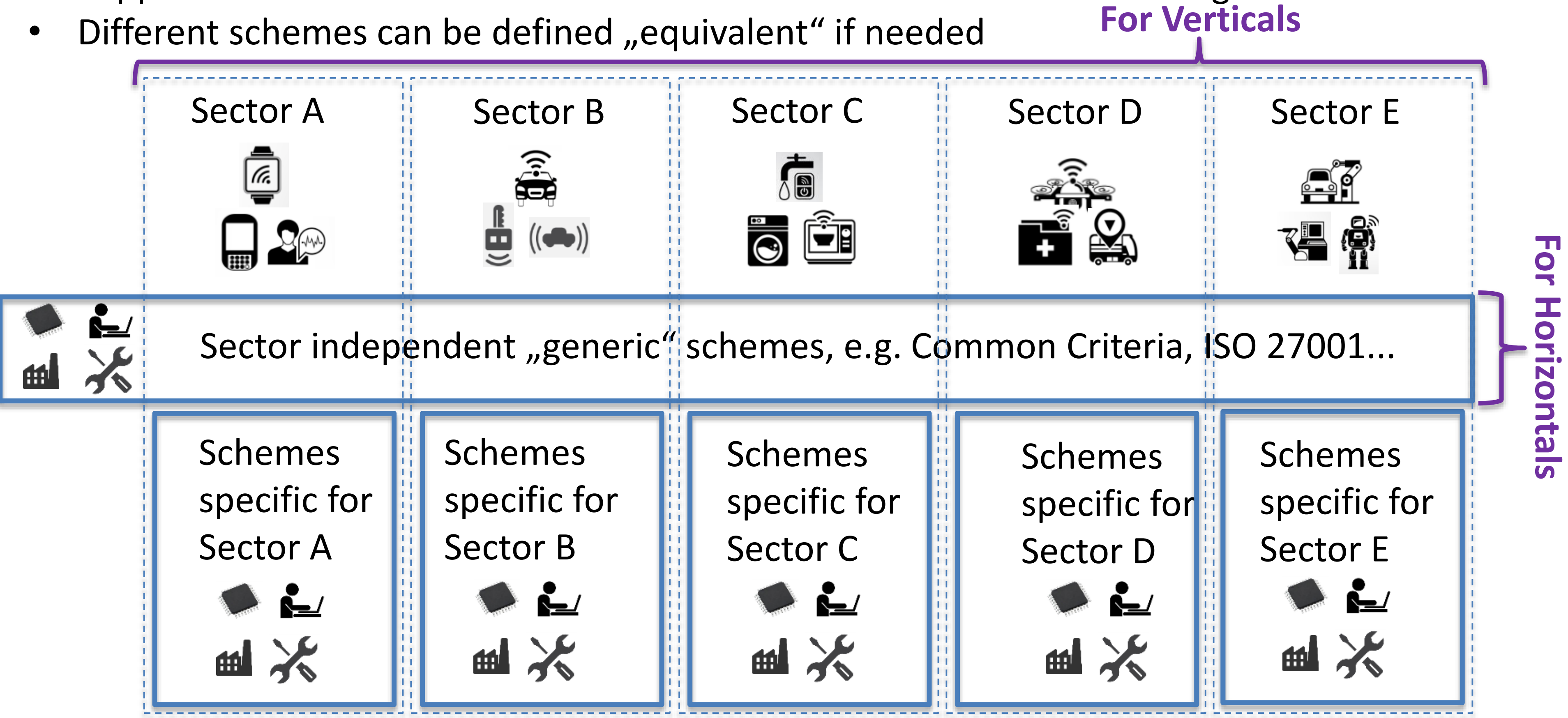
Security professionals

Existing types of certification schemes

Use cases

Meta-Scheme Idea

- Allows composition across **different** schemes via a meta-language
- Supports scaleable common structure and re-use across verticals through horizontals
- Different schemes can be defined „equivalent“ if needed



For Verticals

Sector A

Sector B

Sector C

Sector D

Sector E

Sector independent „generic“ schemes, e.g. Common Criteria, ISO 27001...

For Horizontals

Schemes specific for Sector A

Schemes specific for Sector B

Schemes specific for Sector C

Schemes specific for Sector D

Schemes specific for Sector E

Levels of assurance and assessment types

	Symbol (Example)	Assessment Type	Assurance Level	Scope of Security Functionality Level = min	Scope of Security Functionality > min	Schemes allowed
Advanced	A	Accredited Third Party	High	Sector/Use Case dependent	Sector / Use Case dependent	<mapping from SOTA>
	B	Accredited Third Party	Moderate			<mapping from SOTA>
	C	Accredited Third Party	Enhanced Basic			<mapping from SOTA>
Base	D	Accredited Third Party	Basic	Sector/Use Case agnostic		<mapping from SOTA>
	E	Self	Entry			

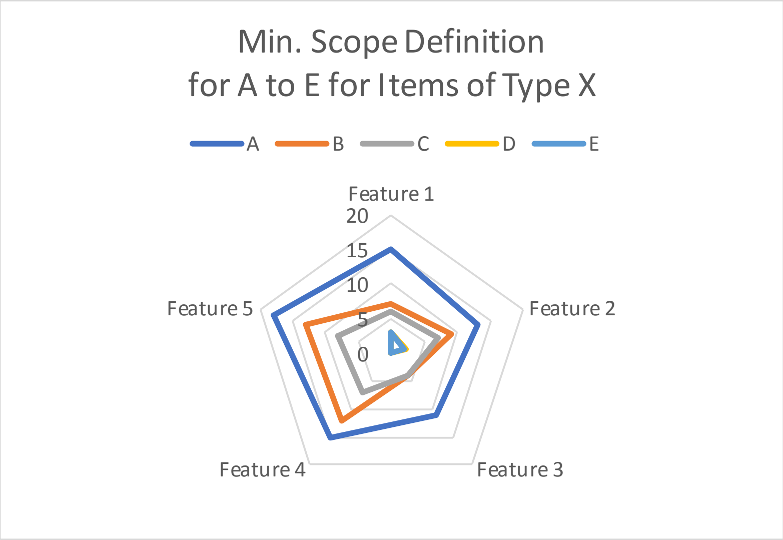
A sector can decide to not define certain levels → free to define if and which advanced levels to provide, whereas the basic levels D and E must be supported in any case

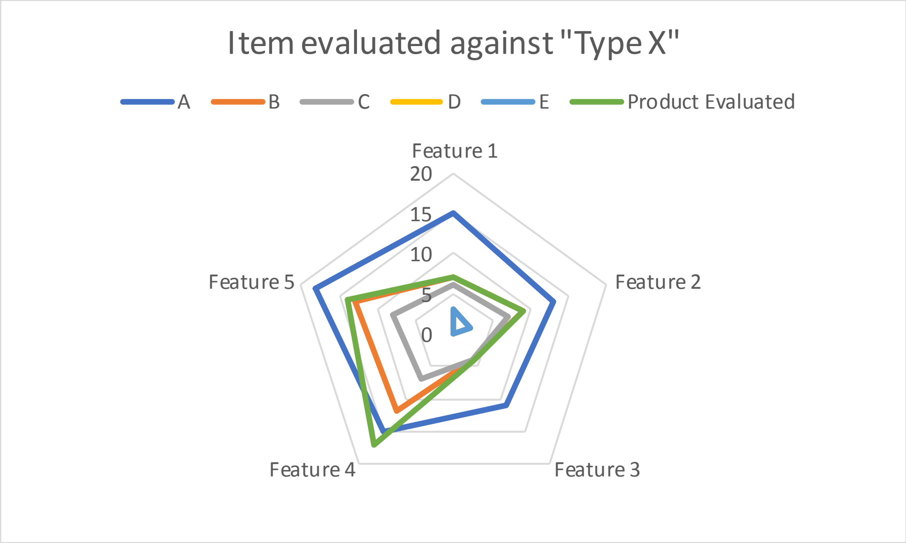
Disclaimer: should be seen as a default case/template for sectors. Depending on the sector this might be refined or overridden in exceptional cases where e.g. assessment by a company-internal independent organisation is done for the advanced levels. Notice, however that this can never replace the level of independence and trust which an external party can give. Moreover, for such cases a very strict shadowing process by an accredited third party is required, which tightly audits the internal organisation on a regular basis. This also has an impact on liability.

Example for a Radar-Diagram to visualize Scope of Security Functionality

Five features defined with their scope of security functionality assessed

The scope of security functionality of the Item evaluated cannot go below the respective claimed line (level A, B, C, D, E) in the radar diagram





This example shall give an understanding that visualization could help a lot to get a feeling on what an item covers.

The Role of Expert Groups

- Experts from Industry, labs, academia, national security agencies, ...
- Definition of **Protection Profiles** (threats/risks → security requirements)
- **Tailoring of evaluation methodologies** (what is „really“ important to look at)
- Maintaining **state-of-the art attack** methods

- Working on **checklists & compliance testing** ...

- ...but also incorporating **Ethical hacking especially for high security!**

Our contribution to the EU Cyber Security Framework

EUROPEAN CYBER SECURITY ORGANISATION

Some conclusions that can be drawn from our work on the EU Cybersecurity Act

- **Experts from industry** part of decision process **for scheme selection and priority –** A roadmap of intended priorities is needed for the market → (The Union Rolling plan will be defined by the SCCG)
- **Minimum common baseline security** needs to be defined **across sectors.** → Threat analysis & risk assessment as source for security requirements
- The **scope of certification** should address the entire supply chain: what and how depends on the intended use
  - The level of assurance attained should consider the potential risk & related impact of potential attacks linked with the product/service usage
- **Ethical hacking shall be legally allowed and enforced for high security**; checklists are insufficient!
- Need for a common definition of the proposed assurance levels, i.e., **assessment methodologies (evaluation) associated**
- **Centrally steered harmonization** across CABs, NABs and National Certification Supervisory Authorities (NCSA) is crucial!

The **ECSO meta-scheme approach** can act as a methodological tool (e.g. for ENISA) to structure the landscape and "glue" existing schemes together and specify additional steps

Current focus

EUROPEAN CYBER SECURITY ORGANISATION

Support to the EU Cybersecurity Certification Framework and Trusted Supply Chain in Europe

- **SOTA, COTI reports update** →Better common understanding of situation and needs to prepare future priorities
- **ECSO Meta-scheme in practice** → Tool for qualitative market analysis to define focused initiatives and promote EU solutions as methodology for the European Certification Framework (identification of the characteristics under which certification schemes can be viewed and selected)
  - New version with general aspects of certification scheme composition, type of evaluations, continuous assessment and a mapping with the Cybersecurity Act
  - Document on Assessment, from self to third-party, looking into the available types of assessment and identifying some of the criteria to decide on the fit-for-purpose type of assessment
- **Analysis of security requirements, gaps in standardization and priorities for future EU certification schemes** → Identify common priorities for definition of certification schemes

Support to EU standardisation on cybersecurity

- **MoU with CEN/CENELEC (and ETSI to be signed).** Definition of priorities for developing EU standards. → Simplify tasks for ESOs to initiate standardisation, in particular linked to certification

BECOME MEMBER!

CONTACT US

European Cyber Security Organisation 10,
Rue Montoyer
1000 – Brussels – BELGIUM

www.ecs-org.eu

Phone:
+32 (0)
27770252

E-mail:
Dr. Roberto G. Cascella
Senior Policy Manager
roberto.cascella@ecs-org.eu

Follow us
Twitter: @ecso_eu