ECS

EUROPEAN CYBER SECURITY ORGANISATION

European Cyber Security Certification: ECSO Meta-Scheme Approach

Slide-Set Version 20180301d

Dr. Martin Schaffer

Director, Head of Security Maturity & Certification, NXP Semiconductors

Member of ENISA’s Permanent Stakeholders Group

ECSO WG1 Chair (on behalf of EUROSMART)

Conference: Towards the EU Cybersecurity Certification Framework, Brussels 1.3.2018

Working Group 1: Standardization, Certification, Labelling and Supply Chain Management

ECS EUROPEAN CYBER SECURITY ORGANISATION

- Launched **October 2016**

- **136 organisations from public and private sector with 276 experts**

- Released **two documents** in december 2017:
  1. State of the Art Syllabus (SOTA) V2
  2. European Cyber Security Certification: A Meta-Scheme Approach V1

Outline

- European Cyber Security Certification: A Meta-Scheme Approach
- Relation of the work to the EU Cyber Security Act

Outline

- **European Cyber Security Certification: A Meta-Scheme Approach**
- Relation of the work to the EU Cyber Security Act

What industry worries about (examples)

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

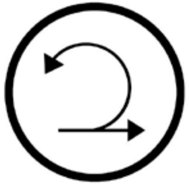
What industry expects (examples)

Fast and predictable

High level of flexibility

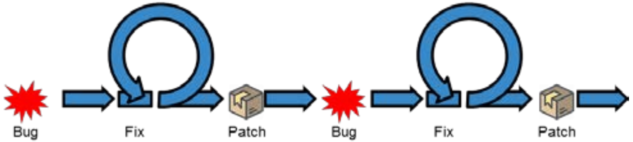
Full harmonization

Pragmatism



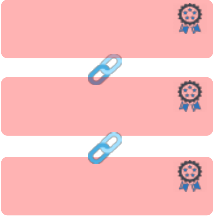
agility

Detecting cheaters in the supply chain



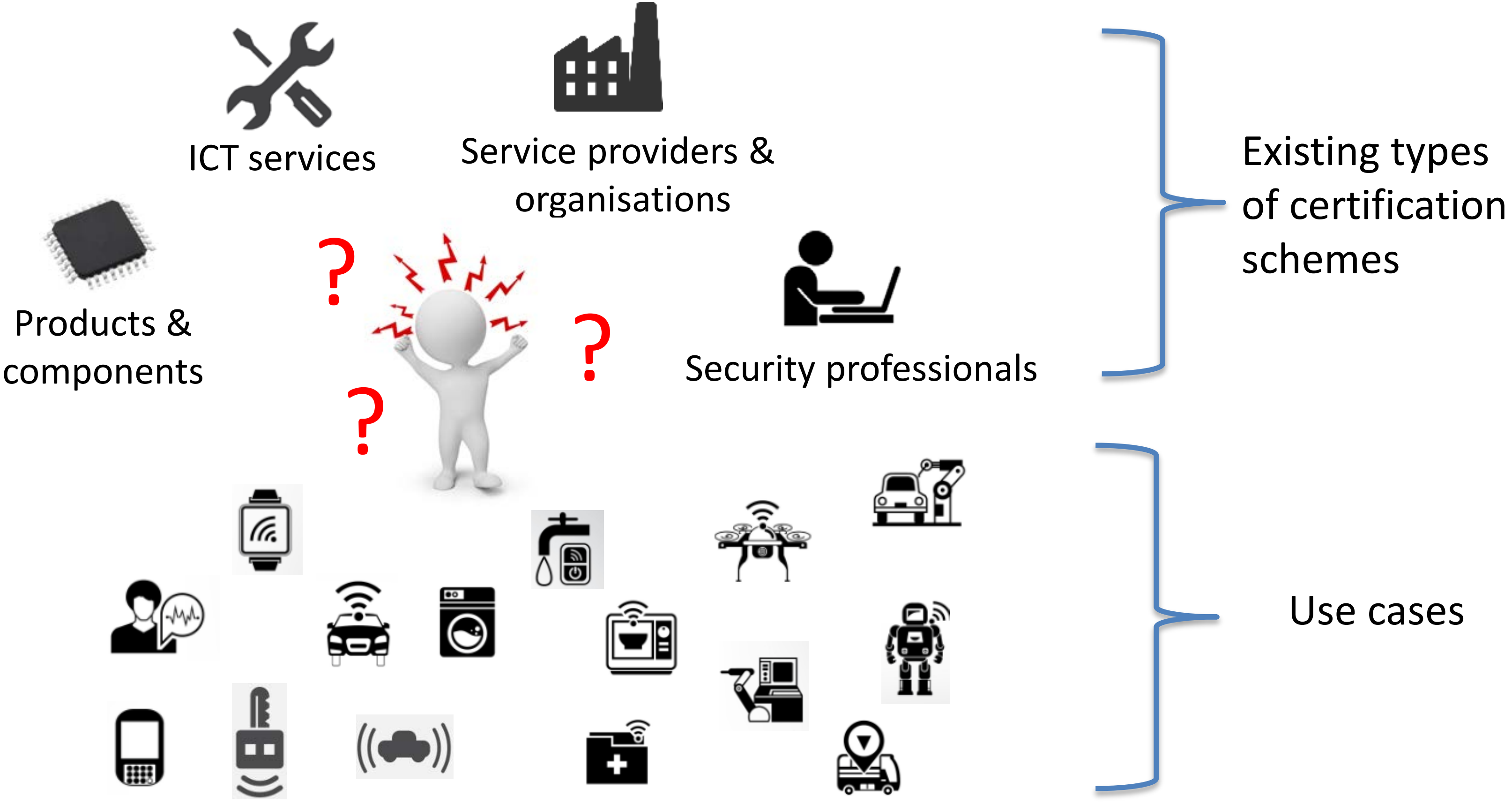
Patching and updates

Ethical hacking



Lean modular composite certifications

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

First of all: collection of what exists!

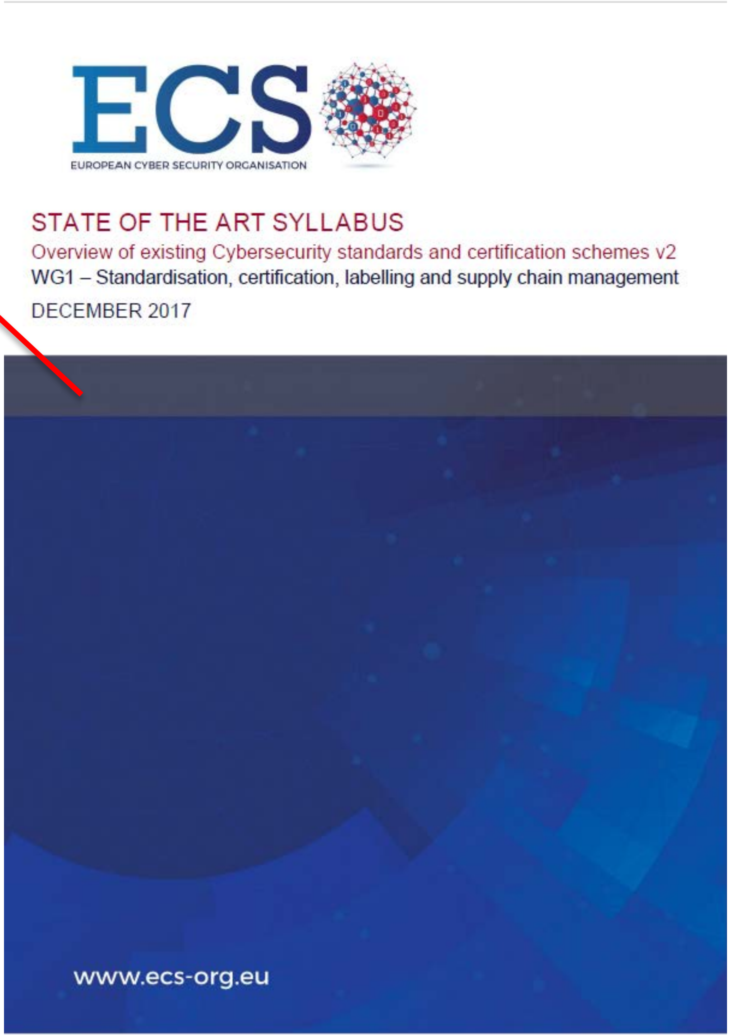
290 standards & schemes

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

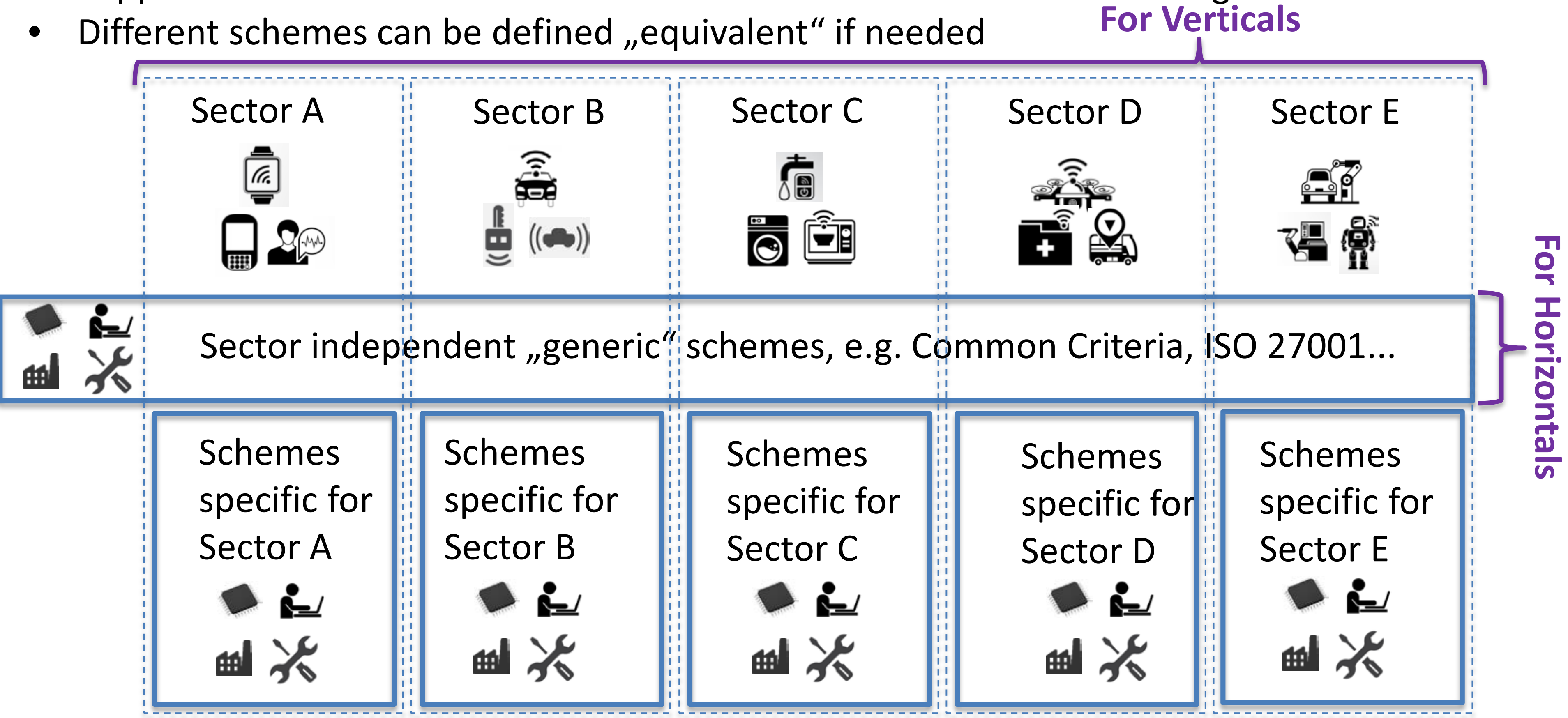
DECEMBER 2017

www.ecs-org.eu

Then create a structure: Meta-Scheme Idea

ECS
EUROPEAN CYBER SECURITY ORGANISATION

- 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...

Schemes specific for Sector A

Schemes specific for Sector B

Schemes specific for Sector C

Schemes specific for Sector D

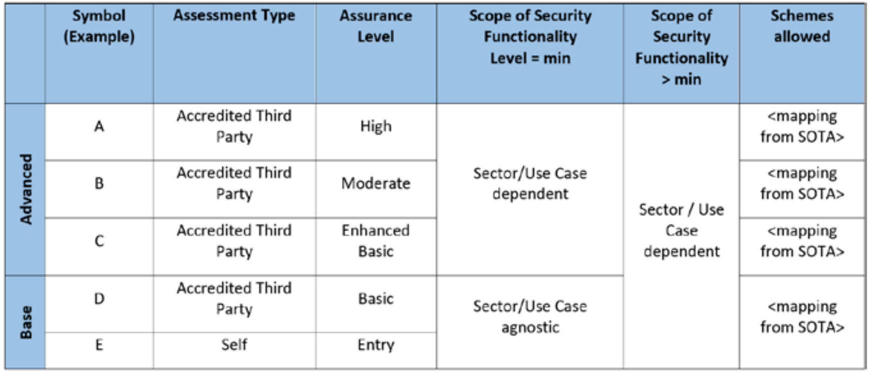
Schemes specific for Sector E

For Horizontals

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			

Identify gaps in the mapped schemes and in the meta-level structure and close them!



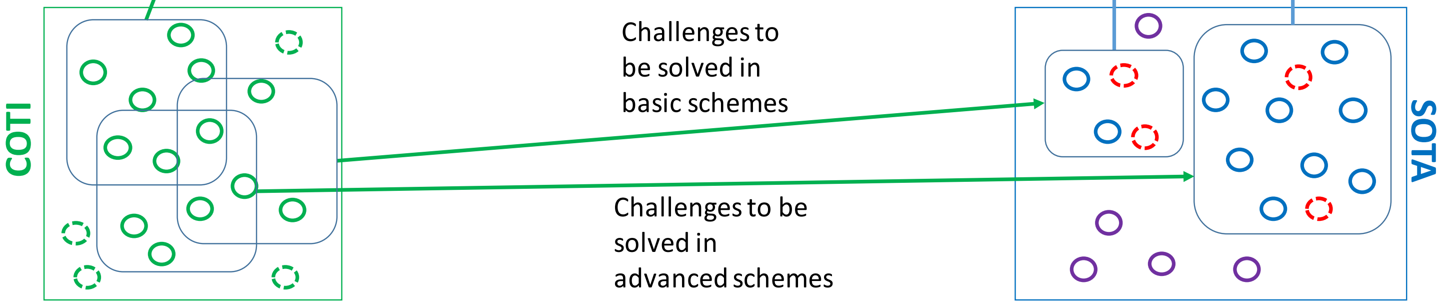
	Symbol (Example)	Assessment Type	Assurance Level	Scope of Security Functionality Level = min	Scope of Security Functionality > min	Schemes allowed
Advanced	A	Accredited Third Party	High	Sector/Use Case dependent	Sector / Use Case dependent	<mapping from SOTA>
	B	Accredited Third Party	Moderate			<mapping 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			

◌ ○ Not applicable
○ ○ applicable
◌ gap

Mapping Schemes appropriate for „advanced“

Mapping and of Schemes appropriate for „basic“

Challenges to be solved in meta-scheme level



Challenges to be solved in basic schemes

Challenges to be solved in advanced schemes

The Role of Expert Groups

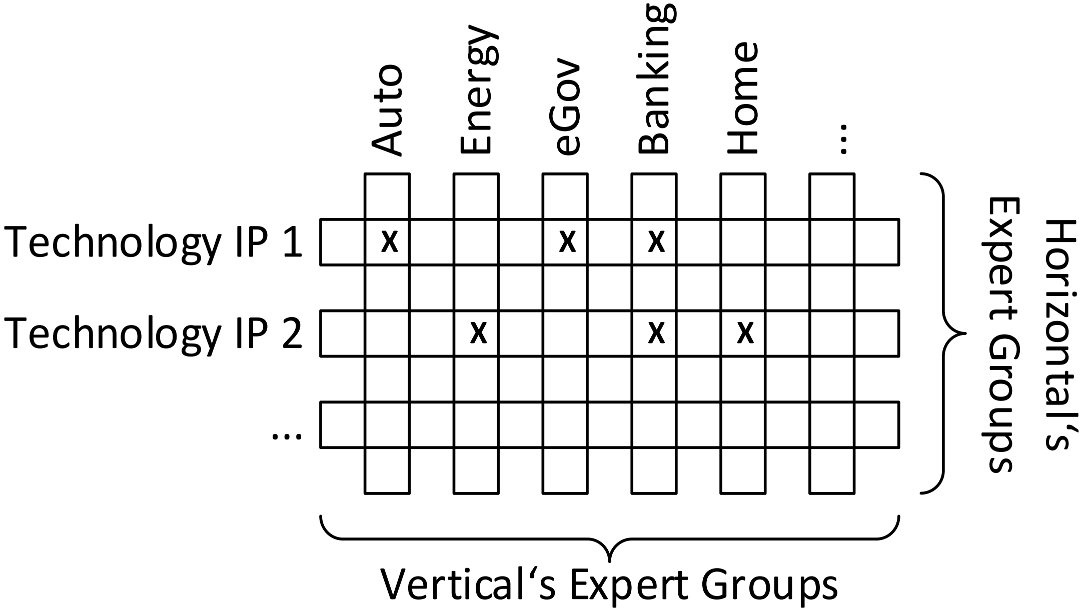
- Experts from Industry, labs, academia, national security agencies, ...
- Definition of **Protection Profiles** (threats/risks → security requirements)
- **Tailoring of evaluation methodologies** (what is „really“ important to look at)
- Maintaining **state-of-the art attack** methods

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

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

The Role of Expert Groups

- **Horizontal View**: experts for a certain technology IP domain
- **Vertical View**: experts for a certain use case doing also risk assessment



	Auto	Energy	eGov	Banking	Home	…
Technology IP 1	X		X	X		
Technology IP 2		X		X	X	
…						

X … Technology IP used by Expert Group of Vertical

Outline

EUROPEAN CYBER SECURITY ORGANISATION

- European Cyber Security Certification: A Meta-Scheme Approach
- **Relation of the work to the EU Cyber Security Act**

Modification Example for EU Cyber Act Levels

Example for adaptions to match EU Cyber Act Levelling

	Symbol (Example)	Assessment Type	EU Cyber Act Levels
Advanced	A^G	National	High
	A	Accredited Third Party	
	B	Accredited Third Party	Subst.
Base	C	Accredited Third Party	Low
	C^S	Self	

We currently develop a proposal to evaluate and determine the level of risk that will determine the need for a certain level of assurance for Products, Services, Organizations and People.

A document will be available in a few days (members of WG1 have access for review and discussion).

Conclusion that can be drawn from our work regarding the EU Cyber Security Act

- **People and organization** certification shall be taken into the scope!
- **Ethical hacking shall be enforced for high security**; checklists are insufficient!
- **Centrally steered harmonization** across CABs, NABs and National Certification Supervisory Authorities (NSCA) is crucial!
- **Experts from industry** shall be part of decision process **for scheme selection and priority**
- Entry **base line security** needs to be defined **across sectors**
- The **meta-scheme approach** can act as a central tool (e.g. by ENISA) to structure the landscape and “glue” existing schemes together and specify additional steps

Please read our 2 released documents!

1. **State of the Art-Syllabus**
   http://www.ecs-org.eu/documents/uploads/updated-sota.pdf

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