The emerging EU certification framework: A role for ENISA

Dr. Andreas Mitrakas | Head of Unit

EU Certification Framework Conference | Brussels | 01/03/18

Background

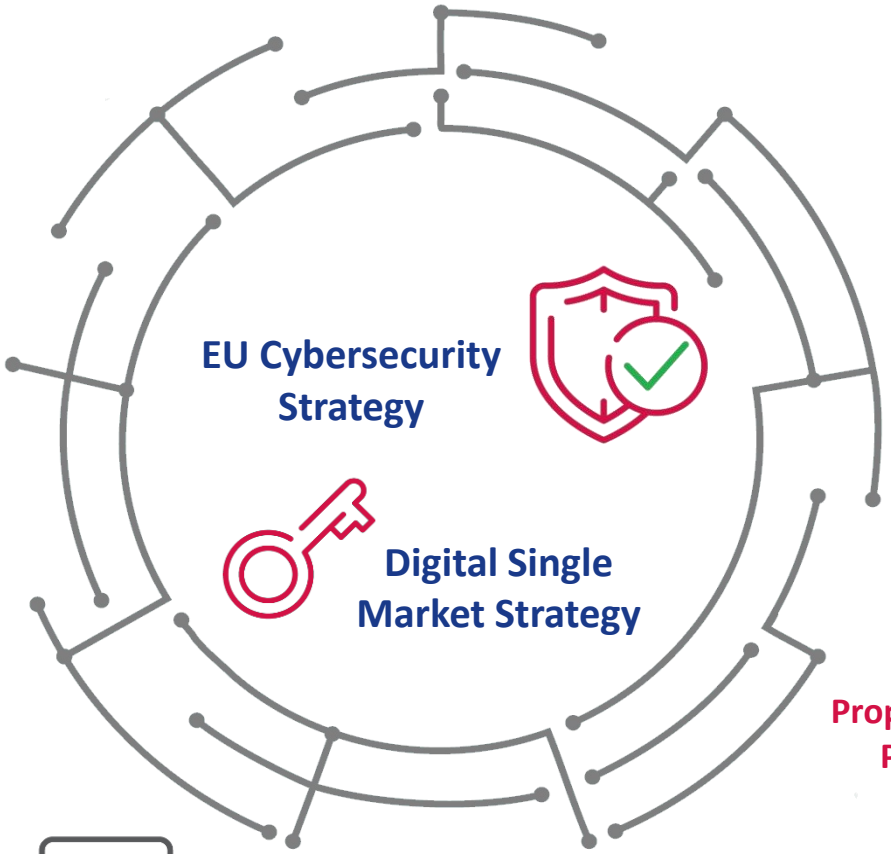
- Defining Certification

" formal evaluation of products, services and processes by an independent and accredited body against a defined set of criteria standards and the issuing of a certificate indicating conformance "(*)

- Security certification of products has been led by the evolution of Common Criteria and work of SOG-IS and private initiatives

(*)EC COM(2017) 477 final

ICT security certification in the EU



Network and Information Security Directive

eIDAS Regulation

Payment Services Directive 2

General Data Protection Regulation

Proposal for a Regulation on Privacy and Electronic Communications

Strengthening Europe's Cyber Resilience System and Fostering a Competitive and Innovative Cybersecurity Industry

The EU certification framework of the Cybersecurity Act

Brussels, 13.9.2017
COM(2017) 477 final

2017/0225 (COD)

Proposal for a

REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

on ENISA, the "EU Cybersecurity Agency", and repealing Regulation (EU) 526/2013, and on Information and Communication Technology cybersecurity certification ("Cybersecurity Act")

(Text with EEA relevance)

{SWD(2017) 500 final}
{SWD(2017) 501 final}
{SWD(2017) 502 final}

Features of an EU certification framework

Member States

ICT Security Certification Producers

ICT Security Certification Consumers

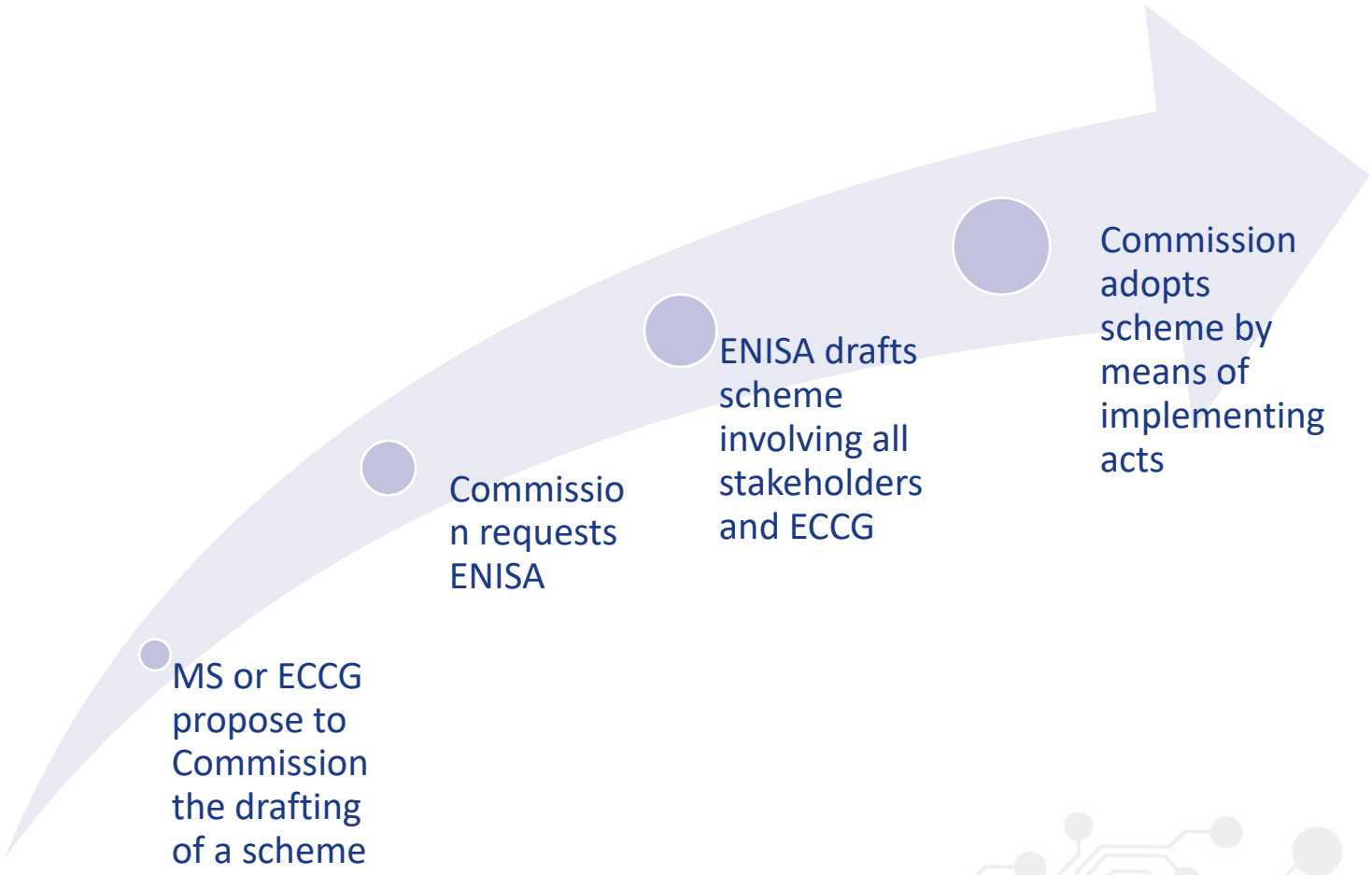
Industry

ECIL Group

ECS EUROPEAN CYBER SECURITY ORGANISATION

- Avoid fragmentation caused by national ICT security certification initiatives
- Promote mutual recognition
- Simplify procedures, reduce the time and cost of deployment of IT products and services
- Improve competitiveness and quality of European products and services
- Give users more confidence in ICT products and services they purchase

EU cybersecurity certification steps



Key elements of a cybersecurity certification scheme

Detailed specification of cybersecurity requirements against which ICT products will be evaluated	**One or more assurance levels**	**Specific evaluation criteria and methods used**	**Information to be supplied to CABs**
Conditions to use marks and labels	**Mechanisms to demonstrate continual compliance as appropriate**	**Conditions to grant maintenance and extension of a certificate**	**Consequences of non-conformity**

ENISA output on certification to date

ENISA certification activities at large

Supporting policy discussions, engagement and dialogue with stakeholders

Establishing working relations with industry working groups

Stocktaking on the development of a European ICT security certification and labelling framework

Analysing the ICT security certification laboratories landscape in the EU

Seeking to engage towards the EU framework based on existing schemes and responding to emerging lightweight requirements

Imprinting the landscape

- Supplementary to community building, involving subject matter experts from Member States and private sector
  - 2013-2014: Cloud certification
  - 2016: Definition of Cybersecurity - Gaps and overlaps in standardisation
  - 2017: Challenges of security certification in emerging ICT environments
  - 2017: Considerations on ICT security certification in EU - Survey Report
  - 2017: Gaps in NIS standardisation - Recommendations for improving NIS in EU standardisation policy
  - 2017: Recommendations on European Data Protection Certification
  - 2018: Overview of the practices of ICT Certification Laboratories in Europe

ENISA in support of the EU Cloud Strategy: Certification

- Strategic objective of EC Strategy: List of voluntary certification schemes
- Cloud Certification Schemes List (CCSL): List of existing certification schemes
  - 13 Certification schemes included
  - Powered by ENISA, supported by the EC and the Cloud Selected Industry Group (C-SIG)

- Cloud Certification Schemes Meta-framework (CCSM): Meta-framework based on existing certification schemes
  - Mapping detailed ICT security requirements of the public sector in the EU (11 countries)
  - Outputs to be used for procurement

Visit: https://resilience.enisa.europa.eu/cloud-computing-certification

An ENISA survey on certification

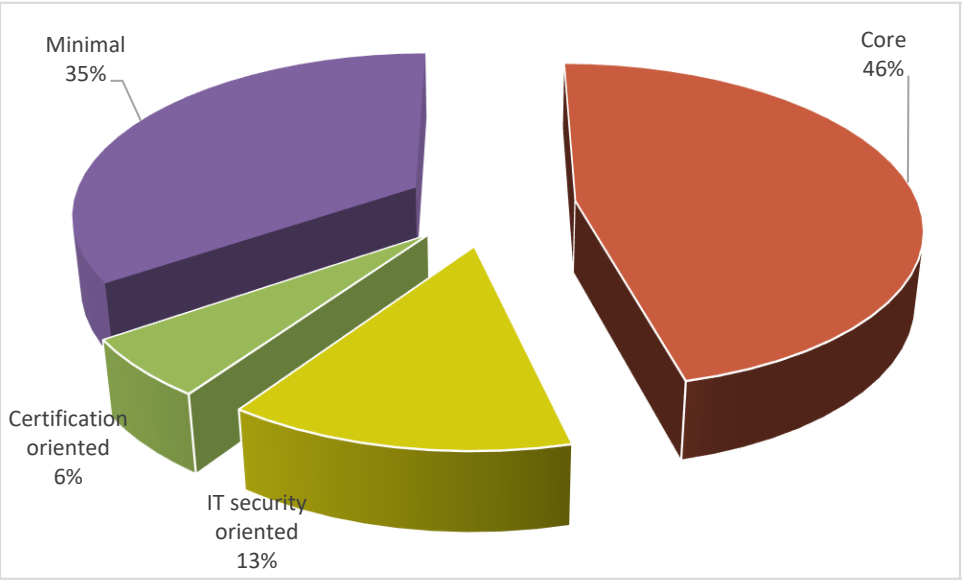
- **57%** is **aware of multiple existing ICT security certification schemes**
- Main **problems** encountered: **costs, duration, transparency and support**
- **90%** agreed that **mutual recognition** is desirable at European level
- **66%** agreed for the need of **self-declaration schemes**
- **Need** for certification and labelling at the **IoT** (**75%**) and **ICS** (**66%**) domains
- **81%** of the respondents agreed also that **certification and labelling can be effective tools** to increase transparency and enhance trust
- **66%** highlighted the need for **greater efforts to promote security certification** in specific sectors
- **78% envisage a role** for the Commission and EU bodies (e.g. JRC, **ENISA**, ACER) in an EU wide approach

EU Conformity Assessment Bodies

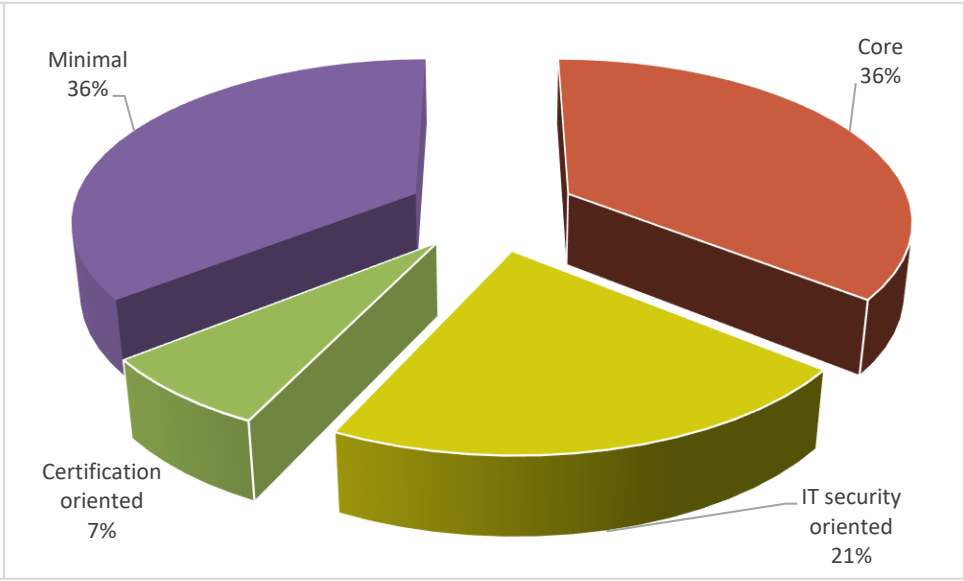
- An ENISA Study analyzing
  - Context of operation
  - Legal framework and standards in the evaluation process
  - Organisation of laboratories and practices thereof

- A few figures
  - 1864 CC certificates in the EU until November 2017
  - On average 100-150 per year

Significance of CC in business

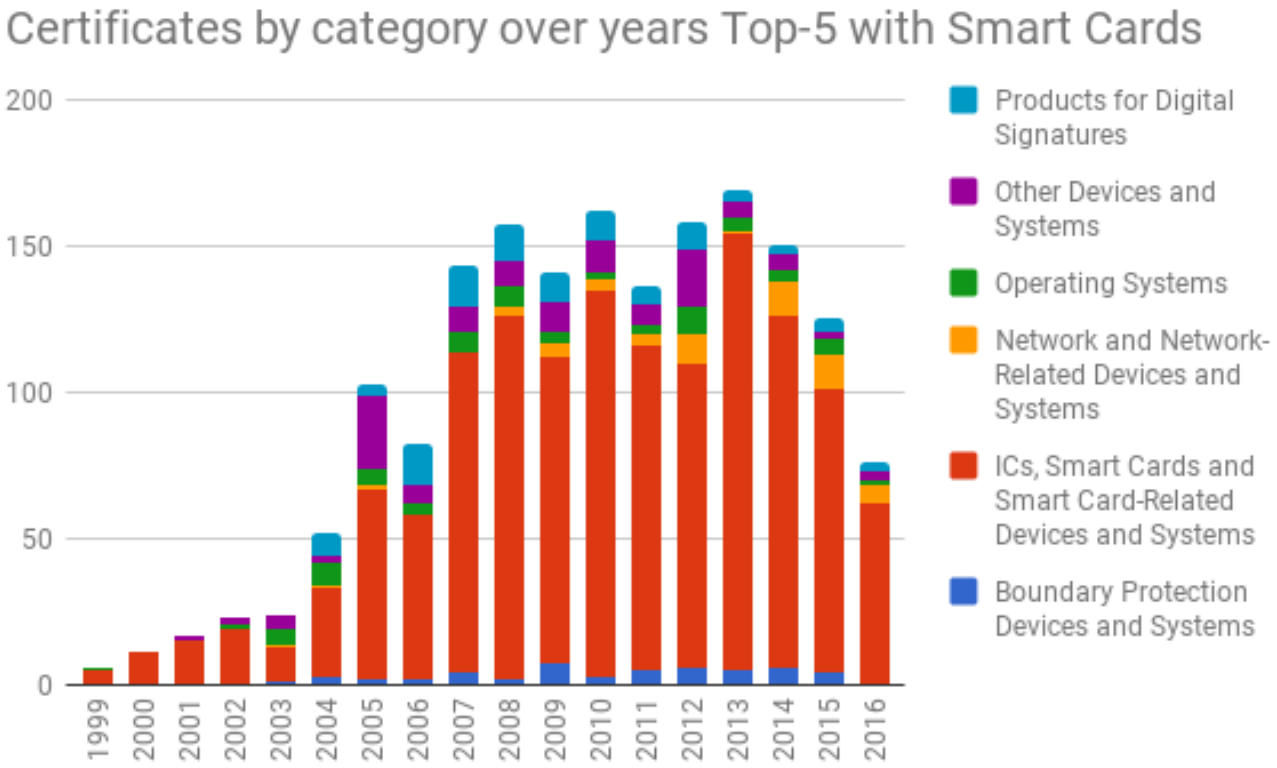


CCRA



SOG-IS

Certificates issued



	2014	2015	2016	TOTAL
Germany	62	46	11	878
Spain	7	7	8	80
France	75	57	57	777
Italy	1	8	3	21
thNetherlands	5	12		45
Sweden	6	7	3	21
UK	7	10	1	41

Standardisation in support of certification

- Standards provide common rules that can be leveraged upon in certification
- Definitions – objects of standards
  - Category of products, services
  - Application needs
  - Requirements
  - Specific security functions
  - Assurance levels
- Evaluation
  - Methodology and process
  - Accreditation of CABs

ENISA-CEN/CENELEC-ETSI workshop

Cybersecurity Act - Establishing the link between Standardization and Certification

13 FEBRUARY 2018 ADD THIS TO MY CALENDAR

THERE IS NO CHARGE FOR THIS EVENT

BRUSSELS, BELGIUM EXPAND

CEN/CENELEC, ENISA and ETSI are organizing a joint workshop on

Shifting ENISA to support the EU certification framework

Envisaged mission of ENISA in certification

To contribute to the emerging EU framework for the certification of products and services and carry out the drawing up of **certification schemes in line with the Cybersecurity Act** providing stakeholders with a sound service that leads to efficiencies and value in the EU

Key outputs

- Key outputs of ENISA Certification include draft and finalised schemes for the certification of products and services, in the meaning of the Cybersecurity Act

Drawing up a certification scheme principles

- **Open**: a scheme to be drawn up by means of open consultations accessible to all parties interested in the technology, products or services affected by the said scheme
- **Consensus seeking**: The consultation process to be collaborative and consensus based refraining from favouring any particular stakeholder
- **Transparent**: Any new scheme activity to be publicised broadly through means available to ENISA. Information concerning technical discussions and consultations to be recorded. Feedback received during the consultation process to be treated in an equitable manner and responses to be provided for

Carrying out certification tasks

ENISA in certification seeks to carry out the following tasks:

- ✓ Stakeholders' coordination
- ✓ Collection of stakeholders' requirements
- ✓ Editing of draft certification schemes
- ✓ Organising and managing scheme drafting activities as projects
- ✓ Management of stakeholders' feedback

Priorities in between

The **primary objectives** of ENISA throughout the period until the Cybersecurity Act comes into force are to:

- *Identify* the **types of certification schemes** in its remit
- *Stimulate* the **interest of stakeholders** in the prospect and opportunity emanating from the EU certification framework
- *Generate* a **list of prospective schemes based on:**
  - **existing ones** seeking to transition to the EU Framework
  - **new application areas** (e.g. consumer), types of products (e.g. IoT) and services (e.g. Cloud)
- *Collect and validate* **stakeholder requirements** in EU certification
- *Make available* the **organisational conditions** to timely fulfil its role

Conclusions

01 Sound preparation of ENISA is underway, during the legislative process

02 Broad stakeholder involvement is seen as a key success factor

03 Internal organisation follows suit

04 Agreeing on principles and content priorities for EU certification schemes are critical steps to take

Thank you

PO Box 1309, 710 01 Heraklion, Greece

Tel: +30 28 14 40 9710

info@enisa.europa.eu

www.enisa.europa.eu