THE EU CYBERSECURITY AGENCY

# The EU Cybersecurity Certification Framework: An Overview

Dr. Andreas Mitrakas
Head of Unit – Data Security & Standardisation, ENISA

Making Software Projects Easier to Understand, The Cube
Athens

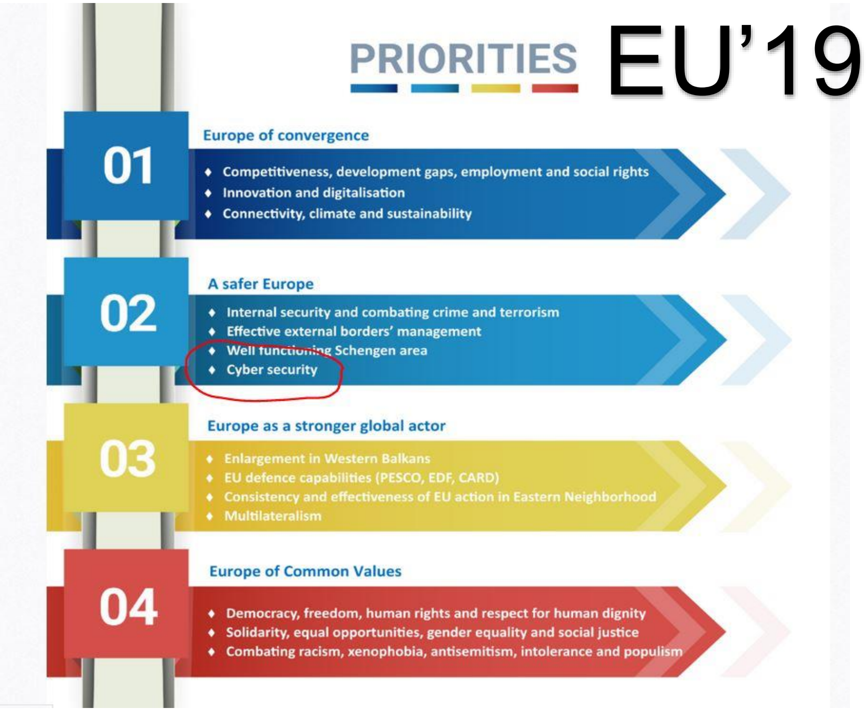
8 05 2019

# AGENDA

## Against a CSA background

## Key processes

## Mission of ENISA



PRIORITIES EU’19

01 Europe of convergence

- Competitiveness, development gaps, employment and social rights
- Innovation and digitalisation
- Connectivity, climate and sustainability

02 A safer Europe

- Internal security and combating crime and terrorism
- Effective external borders’ management
- Well functioning Schengen area
- Cyber security

03 Europe as a stronger global actor

- Enlargement in Western Balkans
- EU defence capabilities (PESCO, EDF, CARD)
- Consistency and effectiveness of EU action in Eastern Neighborhood
- Multilateralism

04 Europe of Common Values

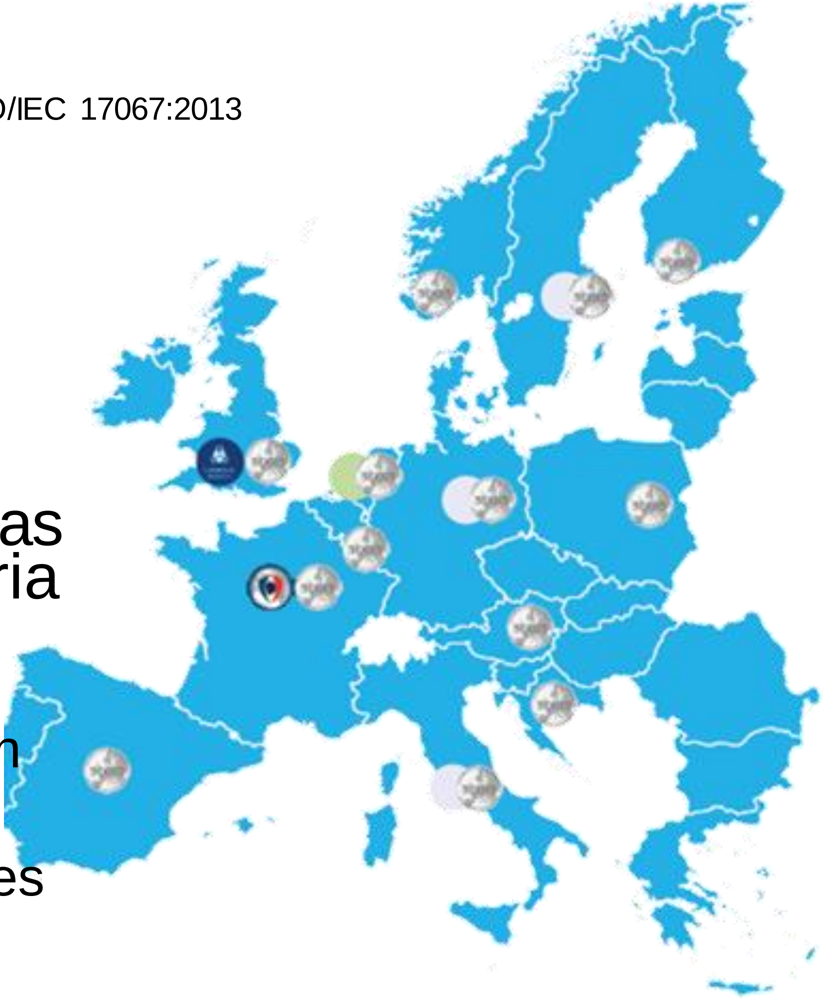
- Democracy, freedom, human rights and respect for human dignity
- Solidarity, equal opportunities, gender equality and social justice
- Combating racism, xenophobia, antisemitism, intolerance and populism

# A CONTINENT IN ACTION

Certification entails

> **"the provision of assessment and impartial third-party attestation that fulfilment of specified requirements has been demonstrated"**(*)

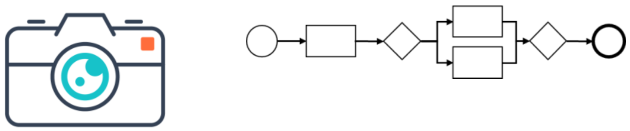
(*) ISO/IEC 17067:2013



- Security certification of products has been tantamount to common criteria
  - Within EU
    - SOG-IS MRA is the forum for common criteria certification
    - Several national and sectorial initiatives focus on security certification

# FAST FORWARD INTO THE FUTURE

## Present



It is challenging to identify if a product/service/process meets specific cybersecurity requirements

Uneven comparison in the absence a common cybersecurity certification framework across all EU MSs

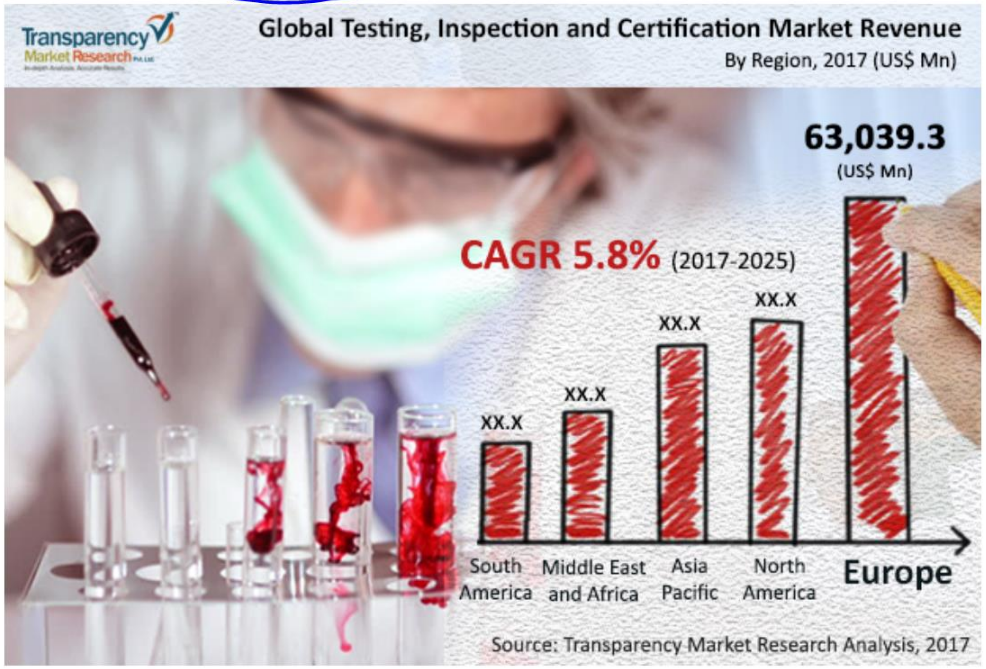
## Future

Straightforward comparison through common levels of assurance

Certification based on a harmonized framework across all EU MSs

# ANOTHER POINT OF VIEW

The global testing, inspection and certification market stood is expected to garner a CAGR of 5.8% during 2017–2025. The market stood at US$184,545.5 million in 2016 and is anticipated to reach worth of US$299,628.6 million by the end of 2025.


Global Testing, Inspection and Certification Market Revenue
By Region, 2017 (US$ Mn)

Source: Transparency Market Research Analysis, 2017

ternet

## of Things to Reach $745 Billion in 2019

Posted by IoT.Business.News | Date: January 03, 2019 | in: Market

# GOALS OF THE CSC FRAMEWORK

- **Addresses market fragmentation**
  - Products, services, processes
- **A risk-based approach for voluntary certification**
  - EU declaration of conformity
- **Defined assurance levels (Basic, Substantial, High)**
- **Role for Member States**
  - Propose the drafting of a candidate scheme
  - Involvement through European Cybersecurity Certification Group (composed of national certification supervisory authorities)
  - Involved in the adoption of an implementing act
- **Tasks outlined as per Regulation (EU) 765/2008 on accreditation and market surveillance**

# KEY PROVISIONS FOR ENISA 1/3

**Prepare candidate schemes or review existing ones, on the basis of:**

The Rolling Work Program (RWP) for EU Cybersecurity Certification

A specific request of the Commission or of the ECCG

**Maintain a dedicated website providing information on:**

EU cybersecurity certification schemes

National certification schemes replaced by EU ones

A store of EU statements of conformance

# KEY PROVISIONS FOR ENISA 2/3

**While carrying out its tasks take into account the requirements on:**

Security objectives of EU cybersecurity certification schemes

Assurance levels

Elements of EU cybersecurity certification schemes

**Participate in the peer review of National Cybersecurity Certification Authorities**

**Assist the Commission to provide secretariat to the ECCG**

**Along with the Commission, co-chair the SCCG**

**Provide secretariat to the SCCG**

# KEY PROVISIONS FOR ENISA 3/3

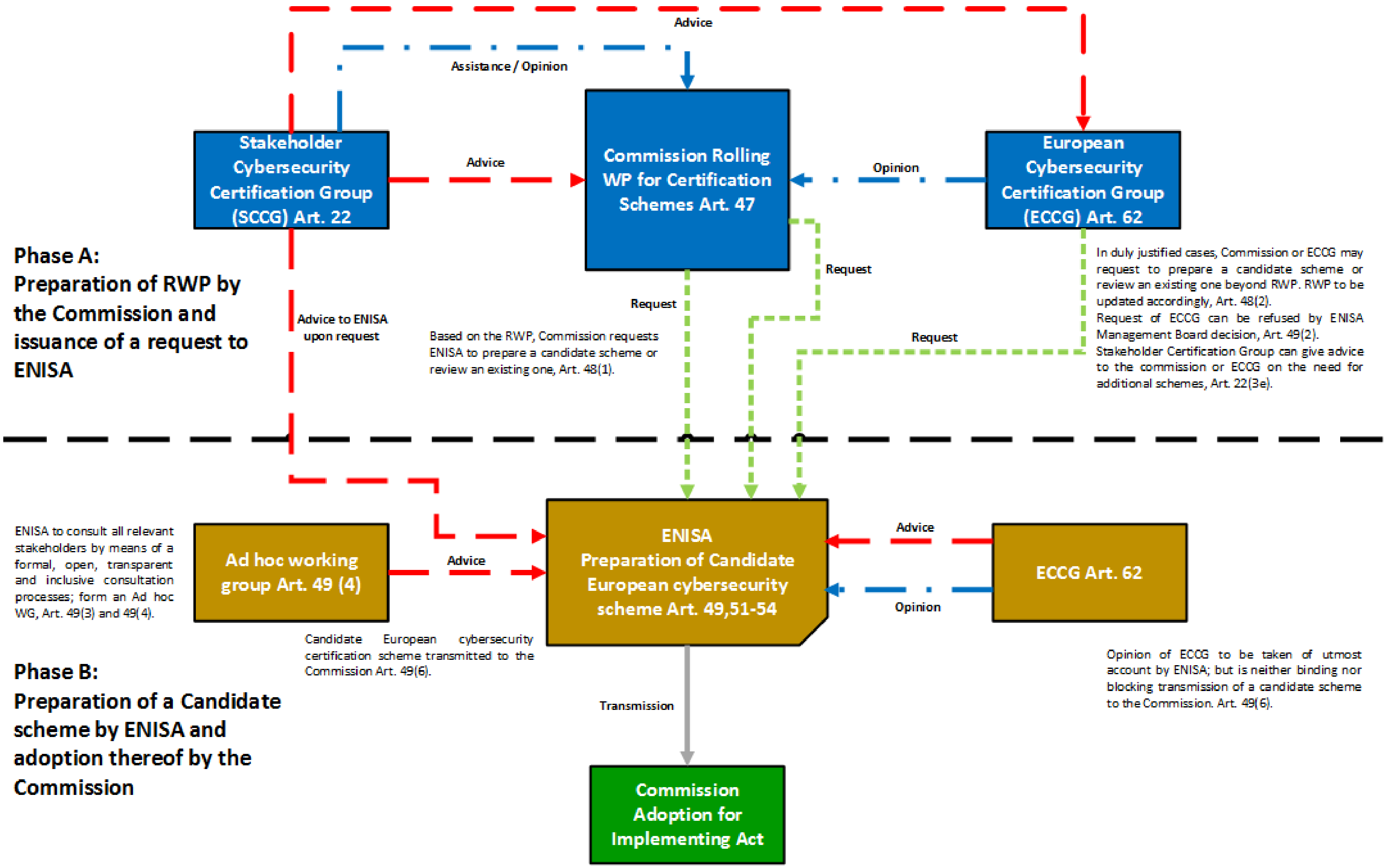
**Additionally, ENISA could potentially provide guidance on such areas as:**

Conformity self assessment

Cybersecurity information for certified products, services and processes

Etc.

# STAKEHOLDERS’ INTERACTIONS



Stakeholder Cybersecurity Certification Group (SCCG) Art. 22

Commission Rolling WP for Certification Schemes Art. 47

European Cybersecurity Certification Group (ECCG) Art. 62

**Phase A: Preparation of RWP by the Commission and issuance of a request to ENISA**

Based on the RWP, Commission requests ENISA to prepare a candidate scheme or review an existing one, Art. 48(1).

In duly justified cases, Commission or ECCG may request to prepare a candidate scheme or review an existing one beyond RWP. RWP to be updated accordingly, Art. 48(2).
Request of ECCG can be refused by ENISA Management Board decision, Art. 49(2).
Stakeholder Certification Group can give advice to the commission or ECCG on the need for additional schemes, Art. 22(3e).

ENISA to consult all relevant stakeholders by means of a formal, open, transparent and inclusive consultation processes; form an Ad hoc WG, Art. 49(3) and 49(4).

Ad hoc working group Art. 49 (4)

ENISA Preparation of Candidate European cybersecurity scheme Art. 49,51-54

ECCG Art. 62

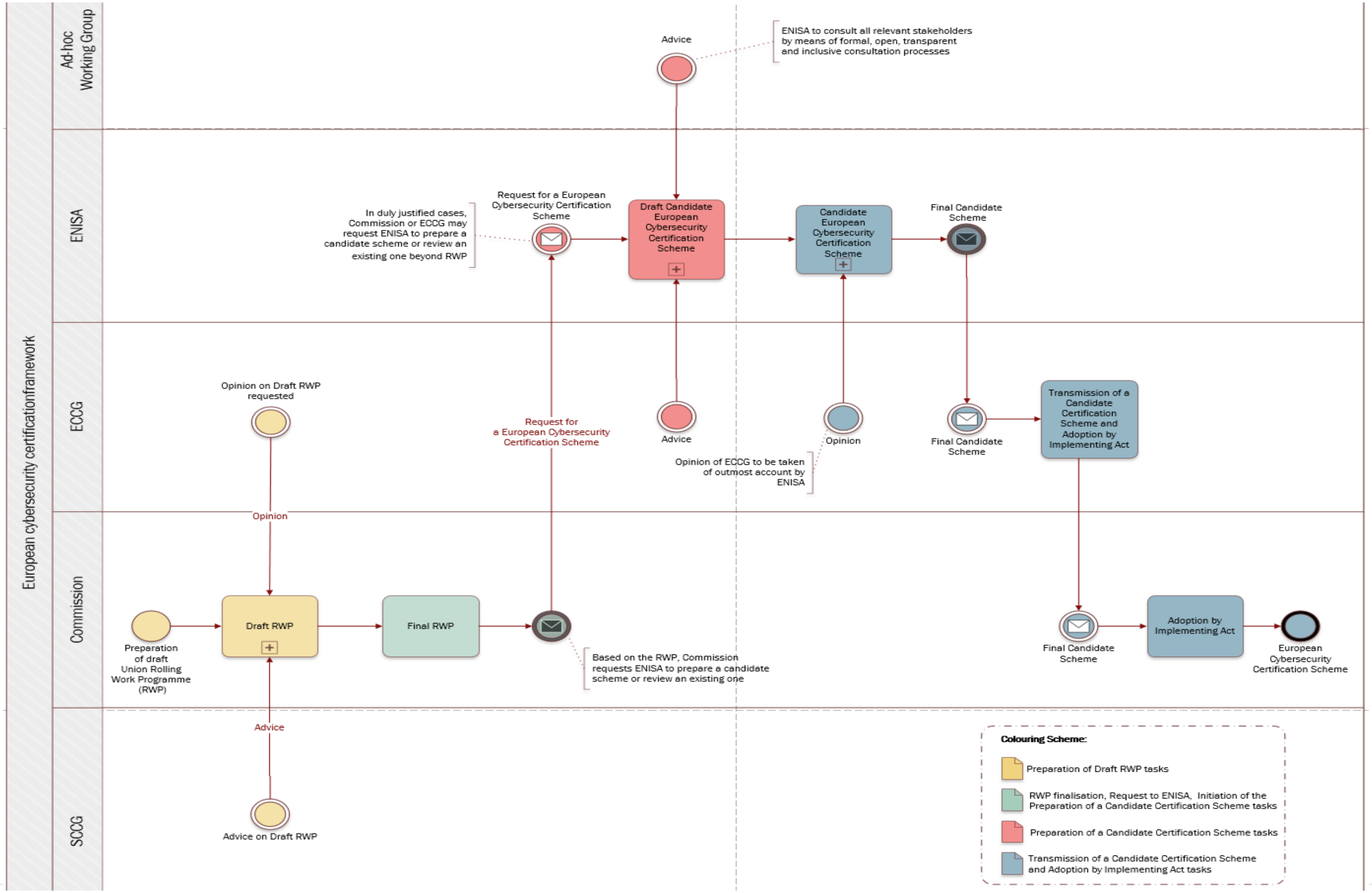
Candidate European cybersecurity certification scheme transmitted to the Commission Art. 49(6).

Opinion of ECCG to be taken of utmost account by ENISA; but is neither binding nor blocking transmission of a candidate scheme to the Commission. Art. 49(6).

**Phase B: Preparation of a Candidate scheme by ENISA and adoption thereof by the Commission**

Commission Adoption for Implementing Act

# STAKEHOLDERS' INTERACTIONS



European cybersecurity certificationframework

Ad-hoc Working Group

ENISA

ECCG

Commission

SCCG

Advice

ENISA to consult all relevant stakeholders by means of formal, open, transparent and inclusive consultation processes

In duly justified cases, Commission or ECCG may request ENISA to prepare a candidate scheme or review an existing one beyond RWP

Request for a European Cybersecurity Certification Scheme

Draft Candidate European Cybersecurity Certification Scheme

Candidate European Cybersecurity Certification Scheme

Final Candidate Scheme

Opinion on Draft RWP requested

Request for a European Cybersecurity Certification Scheme

Advice

Opinion

Opinion of ECCG to be taken of outmost account by ENISA

Final Candidate Scheme

Transmission of a Candidate Certification Scheme and Adoption by Implementing Act

Opinion

Preparation of draft Union Rolling Work Programme (RWP)

Draft RWP

Final RWP

Based on the RWP, Commission requests ENISA to prepare a candidate scheme or review an existing one

Final Candidate Scheme

Adoption by Implementing Act

European Cybersecurity Certification Scheme

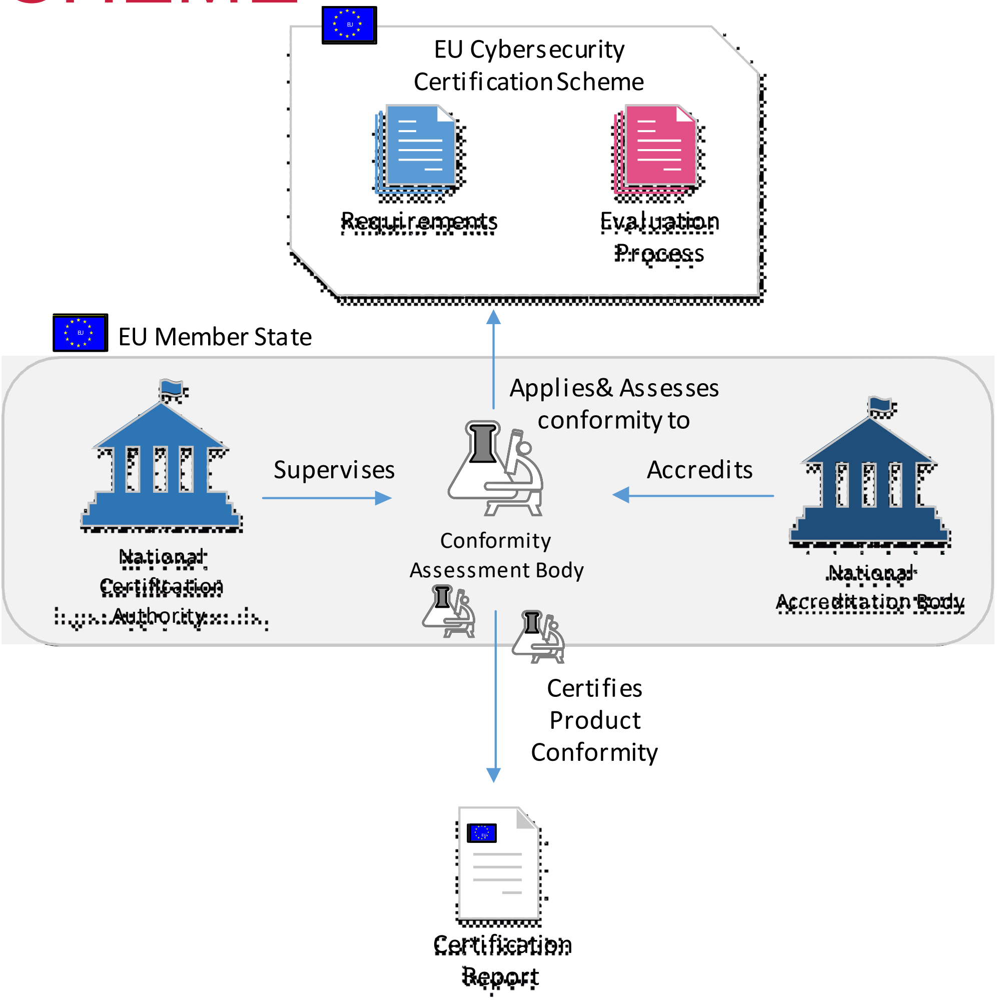
Advice

Advice on Draft RWP

**Colouring Scheme:**

- 🟨 Preparation of Draft RWP tasks
- 🟩 RWP finalisation, Request to ENISA, Initiation of the Preparation of a Candidate Certification Scheme tasks
- 🟥 Preparation of a Candidate Certification Scheme tasks
- 🟦 Transmission of a Candidate Certification Scheme and Adoption by Implementing Act tasks

# CONFORMITY ASSESSMENT AGAINST A CSC SCHEME


EU Cybersecurity Certification Scheme
Requirements
Evaluation Process
EU Member State
Applies& Assesses conformity to
Supervises
Accredits
National Certification Authority
Conformity Assessment Body
National Accreditation Body
Certifies Product Conformity
Certification Report

# MISSION OF ENISA IN THE EU CSCF

To contribute to the emerging EU framework for the certification of products, services and processes

To draw up **certification schemes in line with the Cybersecurity Act** providing stakeholders with a sound service that adds value to the EU while supporting the framework

## Key outputs

- Draft and finalised candidate certification schemes products, services and processes
- Secretariat support (SCCG) and Co-chair SCCG (w/ Commission)
- Support the Commission to Chair ECCG
- Support review of adopted certification schemes
- Implement and maintain CSCF public website
- Support peer review between national cybersecurity certification authorities
- Advice on market aspects relevant to cybersecurity certification

# DEPENDENCIES ON LATERAL POLICY AREAS

## eIDAS

Do we translate it into the new FW at some time?

## NISD

How do we liaise internally? Which areas? OES? -> Link to cooperation group

## GDPR

- As a subject in its own right
- As a horizontal issue

## MDR

- Medical Devices
- SOGIS call

## PSD2

# THANK YOU FOR YOUR ATTENTION

Vasilissis Sofias Str 1, Maroussi 151 24
Attiki, Greece

☎ +30 28 14 40 9711

✉ info@enisa.europa.eu

www.enisa.europe.eu