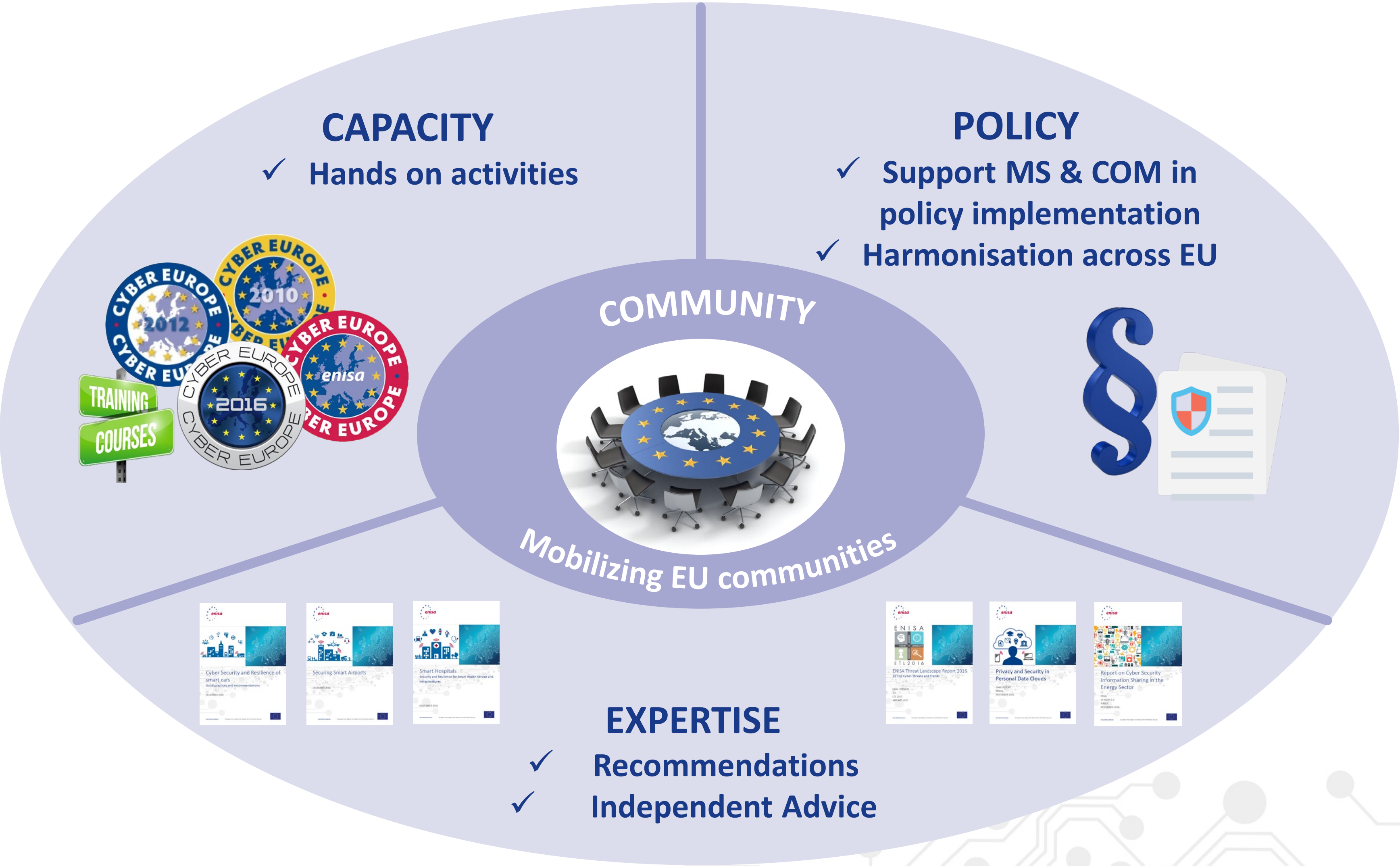
The Cybersecurity Package and the new role of ENISA

CA Day, 24th October 2018

Sławomir Górniak

European Union Agency for Network and Information Security

Positioning ENISA activities



CAPACITY

- ✓ Hands on activities

POLICY

- ✓ Support MS & COM in policy implementation
- ✓ Harmonisation across EU

COMMUNITY

Mobilizing EU communities

EXPERTISE

- ✓ Recommendations
- ✓ Independent Advice

CYBER EUROPE 2012
CYBER EUROPE 2010
CYBER EUROPE enisa
CYBER EUROPE 2016
TRAINING
COURSES
§
Cyber Security and Resilience of smart cars
Securing Smart Airports
Smart Hospitals
ENISA Threat Landscape Report 2016
Privacy and Security in Personal Data Clouds
Report on Cyber Security Information Sharing in the Energy Sector

Cybersecurity Package

Commission President Juncker, State of the EU 2017:

"Cyber-attacks can be more dangerous to the stability of democracies and economies than guns and tanks.

[…]

Today, the Commission is proposing new tools, including a European Cybersecurity Agency to help defend us."

Cybersecurity Package

- **Commission Proposal for a Cybersecurity Act:** *Proposal for a Regulation on ENISA, the "EU Cybersecurity Agency", and on Information and Communication Technology cybersecurity certification (''Cybersecurity Act'') – COM(2017) 477*
- **Renewed Cybersecurity Strategy:** *European Parliament and Council Joint Communication 'Resilience, Deterrence and Defence: Building strong cybersecurity for the EU' (JOIN(2017) 450)*
- **Blueprint:** *Commission Recommendation on Coordinated Response to Large Scale Cybersecurity Incidents and Crises – (C(2017) 6100)*
- **Commission Communication "Making the Most of NIS"** – *towards effective implementation of Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union (COM(2017) 476)*

The Proposed “Cybersecurity Act”

Six key objectives:

1. Increasing **capabilities** and **preparedness** at EU and MS level
2. Improving **cooperation** and **coordination** of stakeholders
3. Increasing EU level capabilities to **complement** MS action
4. Promoting cybersecurity **awareness** in the EU
5. Increasing **transparency** of cybersecurity assurance
6. Avoiding **fragmentation** of certification schemes

The Proposed "Cybersecurity Act"

The proposal contains important new/revised tasks for ENISA:

- **Strengthened and reinforced ENISA; substantially altered:**

  - *Role in policy development and implementation*

  - *Role in operational cooperation – Blueprint*

  - *Participation in research funding programmes*

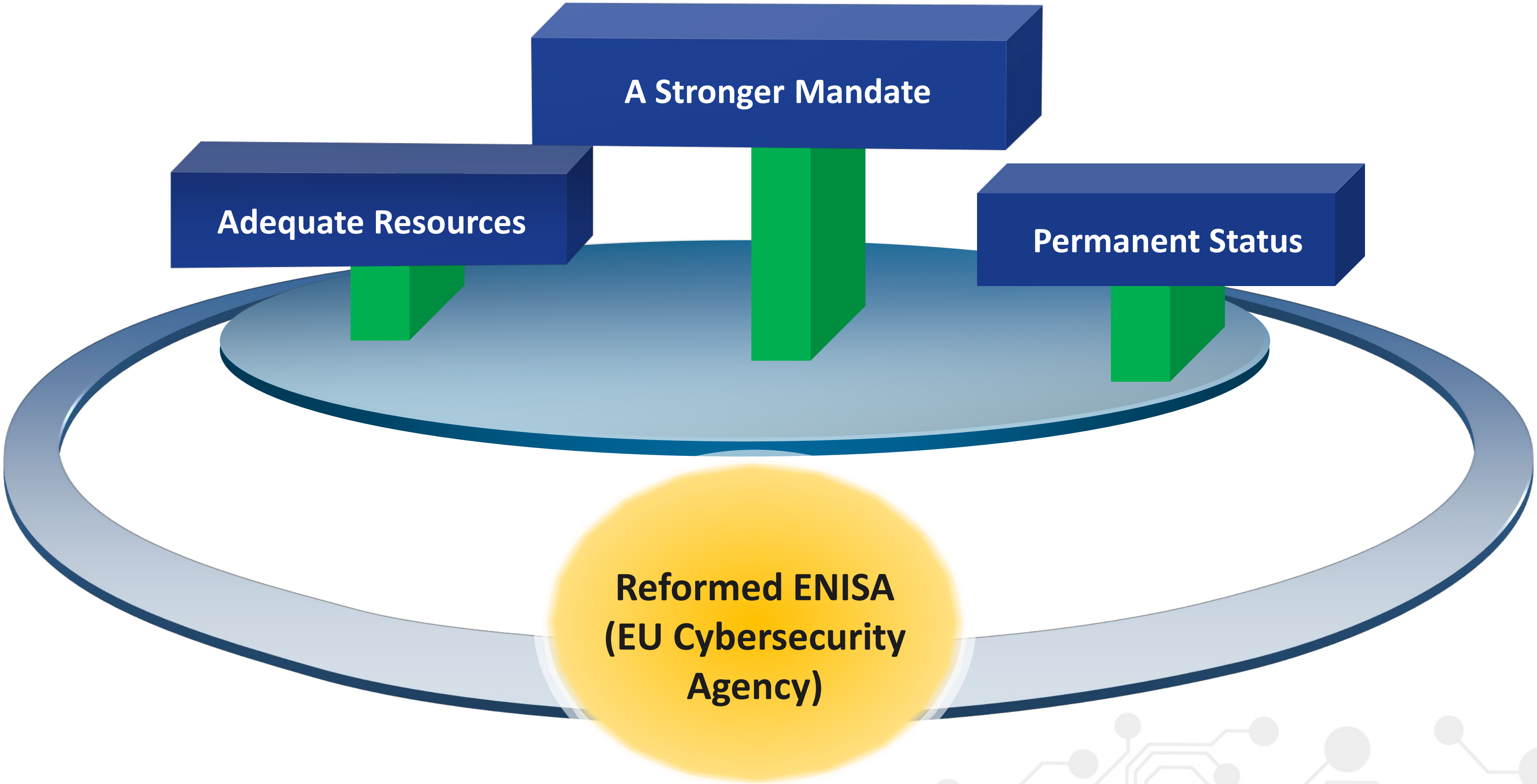
- **EU-level cybersecurity certification framework with:**

  - *A role for ENISA in the preparation of candidate schemes*

  - *Secretariat assistance provided by ENISA for the "European Cybersecurity Certification Group"*

Why ENISA Reform?

- Need for enhanced **role** for ENISA with:



Proposed Tasks for a Stronger ENISA with a **Permanent** Mandate:

Law and Policy Tasks

Capacity Building

Operational Cooperation

Market and Certification

Awareness Raising

Research and Innovation

International Cooperation

EU Cybersecurity Certification Framework Proposal – Background

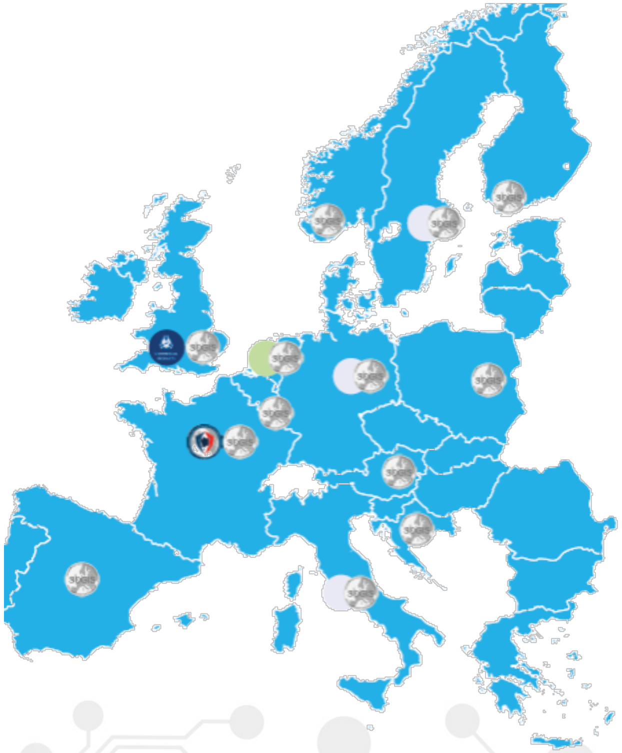
Defining certification:

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

> ***"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"*** (**)

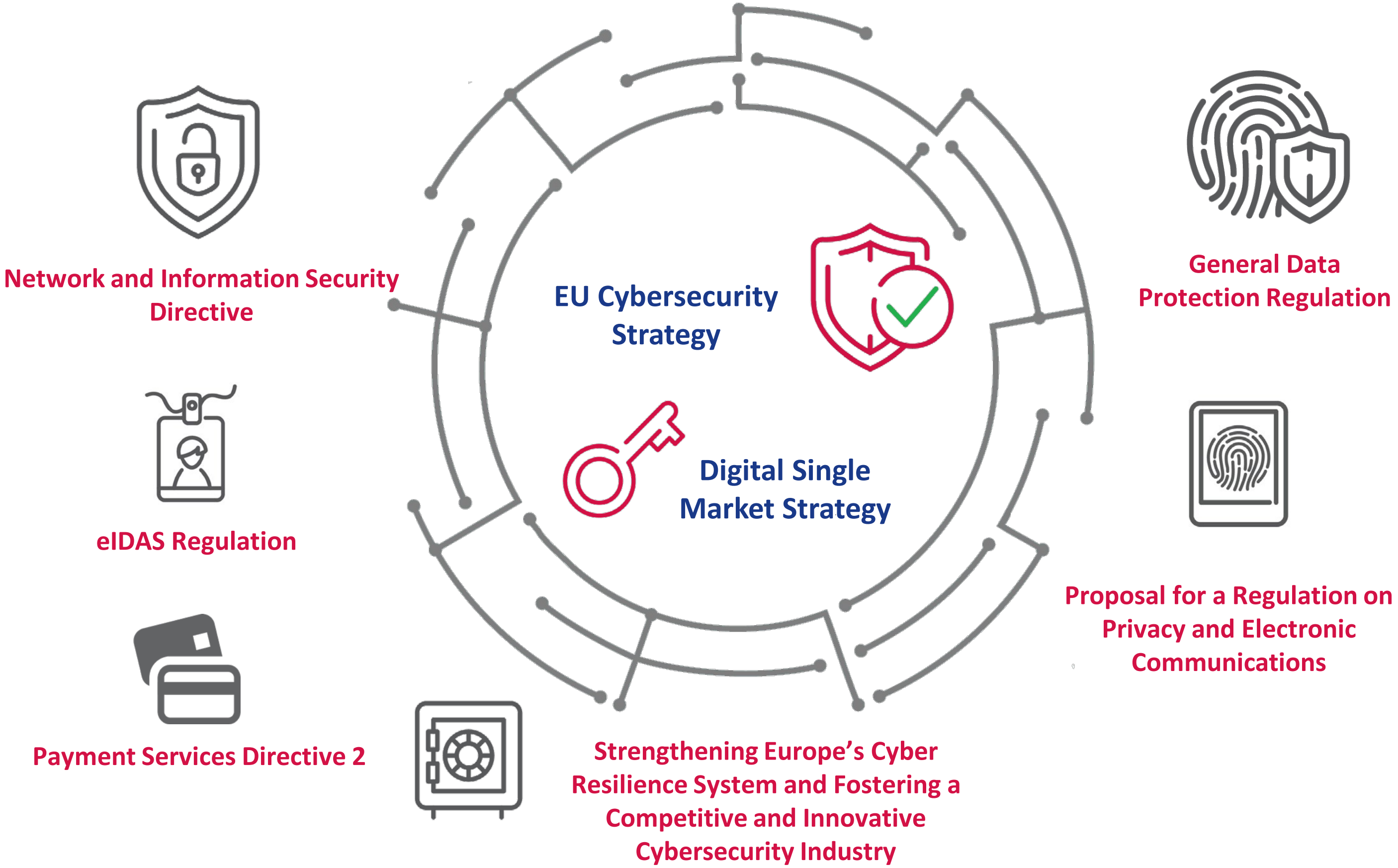
(*) ISO/IEC 17067:2013

(**) EC COM(2017) 477 final



- Security certification of products has been traditionally dominated by Common Criteria
- Within EU
  - SOG-IS MRA is the dominant player in common criteria certification
  - Multiple national and sectorial initiatives focused on security certification

ICT security certification in the EU



EU Cybersecurity Strategy

Digital Single Market Strategy

Network and Information Security Directive

eIDAS Regulation

Payment Services Directive 2

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

Proposal for a Regulation on Privacy and Electronic Communications

General Data Protection Regulation

Possible features of an EU certification framework

ICT Security Certification Producers

ICT Security Certification Consumers

Member States

Industry

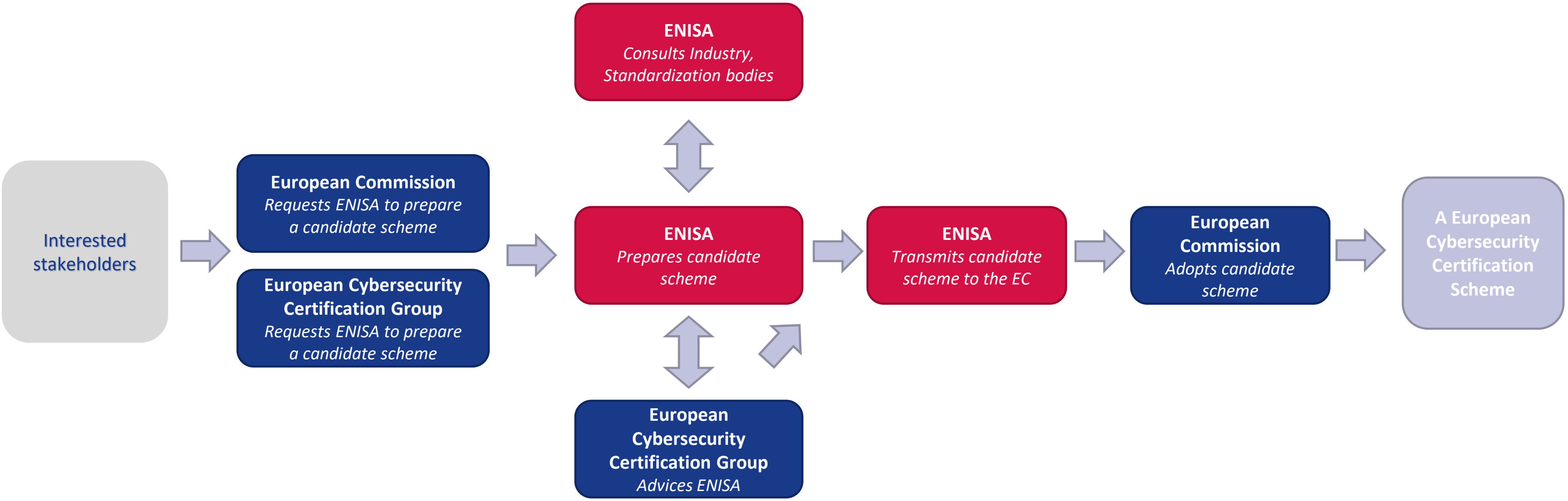
ECIL Group

ECS

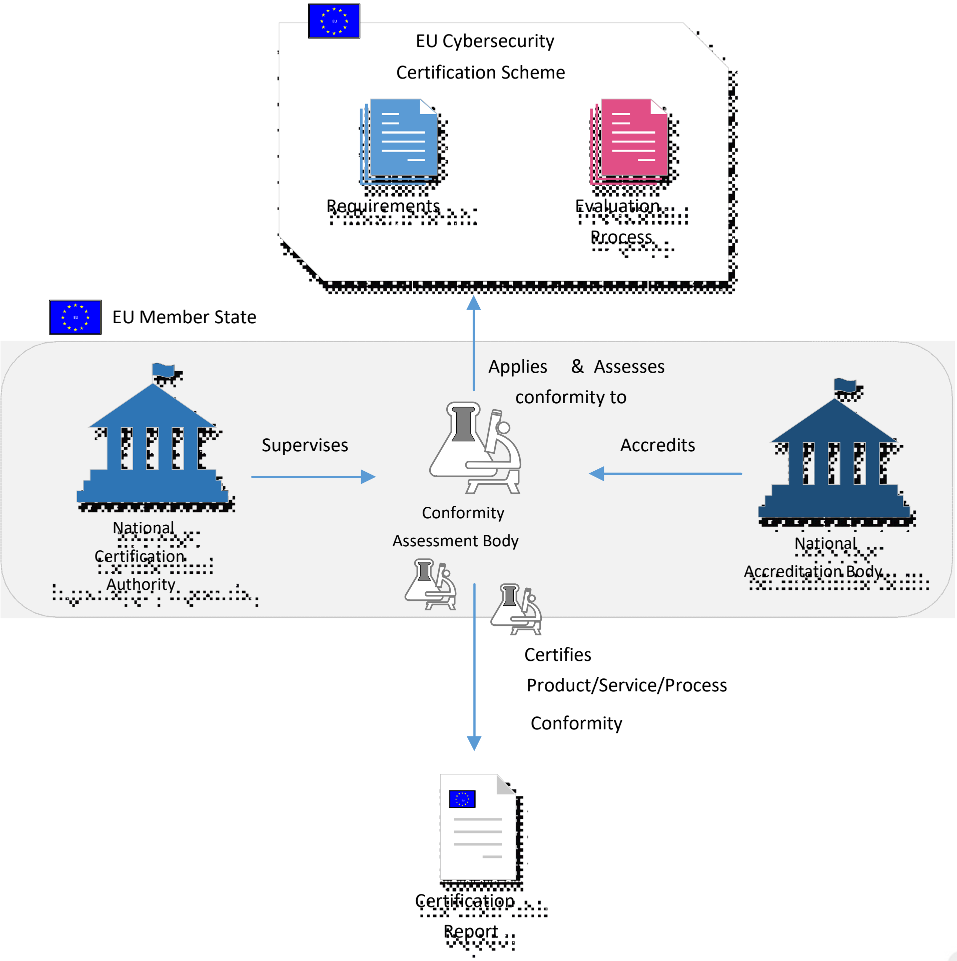
EUROPEAN CYBER SECURITY ORGANISATION

- Avoid fragmentation caused by national ICT security certification initiatives
- Promote mutual recognition
- Defined assurance levels (Basic, Substantial, High)
- 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

Putting certification schemes forward


Interested stakeholders
European Commission *Requests ENISA to prepare a candidate scheme*
European Cybersecurity Certification Group *Requests ENISA to prepare a candidate scheme*
ENISA *Consults Industry, Standardization bodies*
ENISA *Prepares candidate scheme*
European Cybersecurity Certification Group *Advices ENISA*
ENISA *Transmits candidate scheme to the EC*
European Commission *Adopts candidate scheme*
A European Cybersecurity Certification Scheme

Putting certification process forward



Key elements of the proposed framework

Scheme scope including: type and categories of processes, products and services covered	Reference to standards followed in the evaluation process One or more assurance levels	Specific cybersecurity requirements for CABs as appropriate Specific evaluation criteria and methods used	Information to be supplied to CABs by applicant
Conditions to use marks and labels Conditions to grant maintain and extend a certificate	Rules for monitoring compliance of the certificates or the EU declaration of conformity	Rules to report vulnerabilities Records keeping in CABs Identification of national/intl schemes in the same area	Content of issued certificate or EU declaration of conformity Period of validity Disclosure policy Mutual recognition

Drawing up the promulgation of a certification scheme

- **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

Current ENISA certification activities

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

Messages to take away

- The Cybersecurity Package is an important step in assuring resilience of European networks
- ENISA with a new mandate will stronger suport European cybersecurity
- The new ICT security certification framework will improve competitiveness and quality of European ICT products and provide for more confidence
- ENISA will actively contribute to the certification framework

Thank you

PO Box 1309, 710 01 Heraklion, Greece

Tel: +30 28 14 40 9710

info@enisa.europa.eu

www.enisa.europa.eu