Resilience, Deterrence and Defence: Building strong cybersecurity for the EU

EU Cybersecurity Act - Establishing the link between Standardization and Certification

	Building EU Resilience to cyber attacks	Creating effective EU cyber deterrence	Strengthening international cooperation on cybersecurity
Cybersecurity Act	Reformed ENISA	Identifying malicious actors	Promoting global cyber stability and contributing to Europe's strategic autonomy in cyberspace
	EU cybersecurity Certification Framework	Stepping up the law enforcement response	Advancing EU cyber dialogues
Communication	NIS Directive Implementation	Stepping up public-private cooperation against cybercrime	Modernising export controls, including for critical cyber-surveillance technologies
Recommendation	Rapid emergency response – Blueprint & Cybersecurity Emergency Response Fund	Stepping up political and diplomatic response	Continue rights-based capacity building model
	Cybersecurity competence network with a European Cybersecurity Research and Competence Centre	Building cybersecurity deterrence through the Member States' defence capabilities	Deepen EU-NATO cooperation on cybersecurity, hybrid threats and defence
	Building strong EU cyber skills base, improving cyber hygiene and awareness		

EU Cybersecurity Act

Towards a reformed EU Cybersecurity Agency and reinforcing the cybersecurity single market in the EU

ENISA

Towards an EU Cybersecurity Agency fit for current and future challenges

Market

Cybersecurity Certification Framework

- preparing candidate European cybersecurity certification schemes
- assist the Commission in providing the secretariat to the European Cybersecurity Certification Group
- guidelines and developing good practices concerning the cybersecurity requirements of ICT products and services

Standardisation

- facilitate establishment & take-up of EU & international standards for risk management and for the security of ICT products &services
- advice and guidelines related to the security requirements for OES and DSPs, as well as regarding already existing standards (NIS-D art. 19)

Market Observatory

- analyses on trends of cybersecurity market (demand and supply sides)

ICT cybersecurity certification

Towards a true cybersecurity single market in the EU

The issue

- The **digitalisation** of our society generates greater need for cyber secure products and services

- Cybersecurity certification plays an important role in **increasing trust** of digital products and services

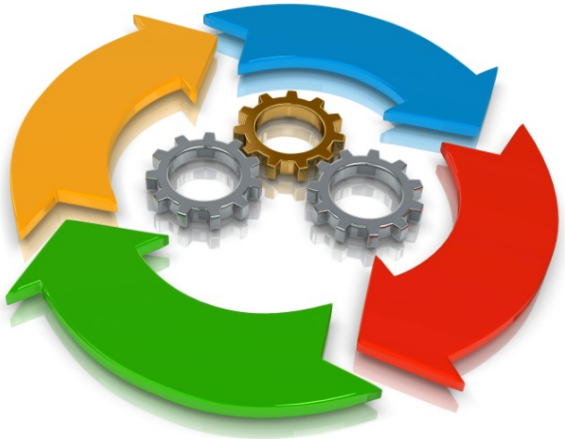
Current landscape

  - emergence of separate national initiatives lacking mutual recognition (e.g. France, UK, Germany, Netherlands, Italy)

  - SOG-IS MRA successful
    - membership (14 MSs)
    - costs and duration may not suitable for all market needs

Our proposal

A **voluntary European** cybersecurity certification **framework….**



*…to enable the creation of **tailored** EU cybersecurity certification **schemes** for ICT products and services…*

*…that are **valid across the EU***

Benefits... for **citizens / end users**

NOW

Difficult to distinguish between more and less secure products/services

Co-existence of schemes makes comparison difficult...

...end-users (OES) refrain from buying certified products/services

FUTURE

more information on the security properties of product/services ahead of purchase

Greater incentive for OES to buy certified products/service

Increased cyber resilience of critical infrastructures

...As end-users of digital solutions, governments would rely on an institutional framework to identify and express priority areas needing ICT security certification.

...For vendors/providers

- The possibility to obtain cybersecurity certificates that are valid across the EU would:
  - *Generate higher incentive to certify and enhance the quality of digital products/services*
  - *Enhance competitiveness through reduced time and cost of certification*
  - *Help gain access to market segments where certification is required*
  - *Contribute to promote a chain* of *trust between vendors* and *end-users*
- For **SMEs** and **new business…**
  - *Elimination of a potential market-entry barrier*

Core elements

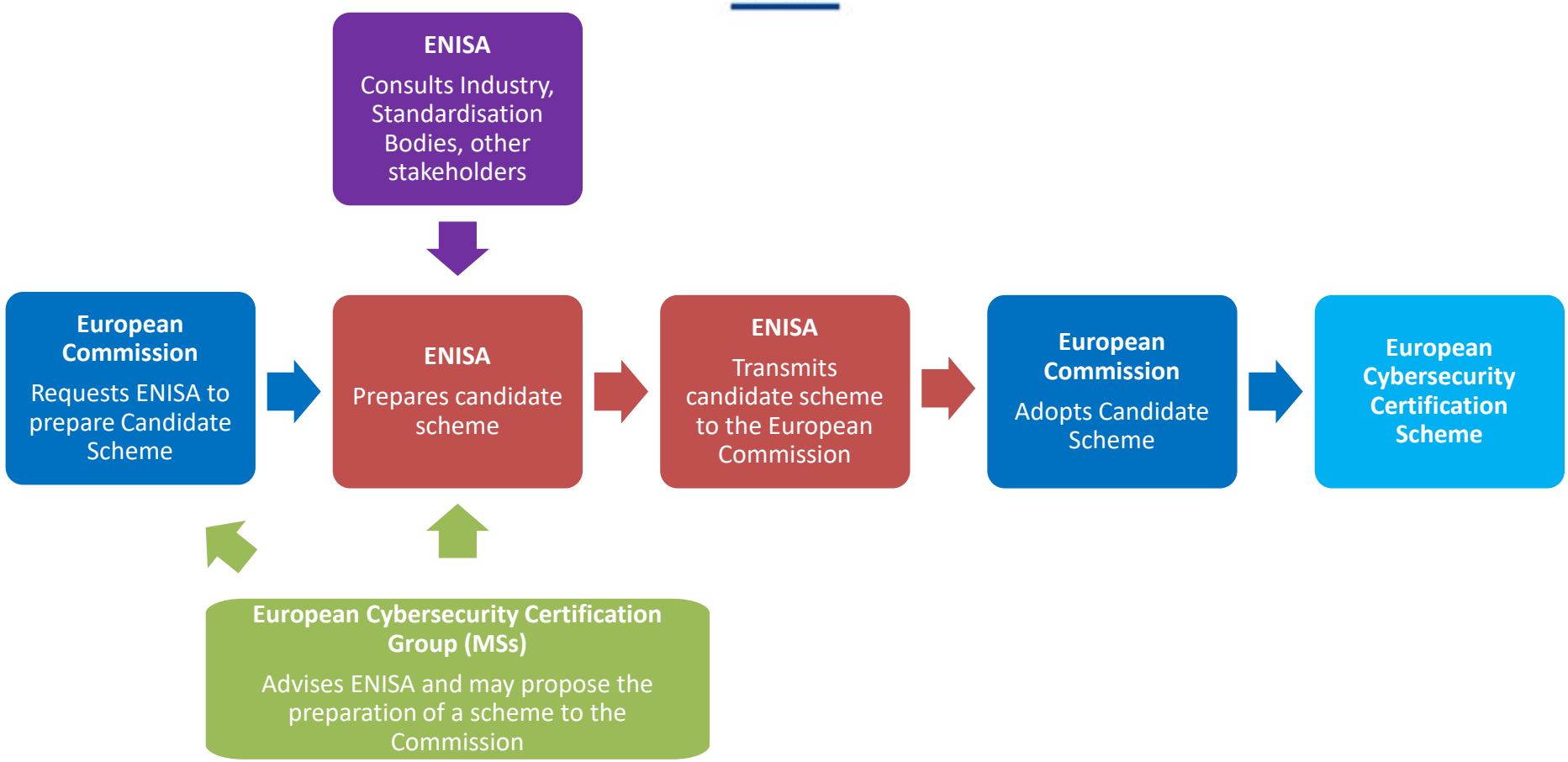
- One EU Cybersecurity Certification Framework, **many** schemes.

- Tailored schemes specifying:
  i. The scope of certification; a product/service or a category of products or services
  ii. Evaluation criteria and security requirements
  iii. Assurance level

- Resulting Certificates from European schemes are valid across all Member States.

- Once a European scheme has been established:
  – Member States cannot introduce new national schemes with same scope
  – Existing national schemes covering same product/service cease to produce effects
  – Existing certificates from national schemes are valid until expire date

- The use of EU certificates remains voluntary, unless otherwise specified in European Union law.
- The specified requirements of the scheme shall not contradict any applicable legal requirements, in particular requirements emanating from harmonised Union legislation.



Overview Establishment of an EU Cybersecurity Certification Scheme

The important role of standards

- Standards are a central element in schemes as they may express both the security requirements as well as the evaluation or assessment methodology used to determine their fulfilment.

- Captured in Article 47 *Elements of European cybersecurity certification schemes*

  – Par. 1 (b): "detailed specification of the cybersecurity requirements against which the specific ICT products and services are evaluated, for example by reference to Union or international standards or technical specifications";
  – Par. 1 (d): "specific evaluation criteria and methods used, including types of evaluation, in order to demonstrate that the specific objectives referred to in Article 45 are achieved";

The important role of standards

- During the preparation of the proposal, we identified well-known standards used in existing certification schemes.
  - The Common Criteria for Information Technology Security Evaluation (CC) - ISO/IEC 15408 Information technology -- Security techniques -- Evaluation criteria for IT security and others
  - IEC 62443 (Industrial communication networks - Network and system security - Part 3-3: System security requirements and security levels)
- Subsequent work has provided more complete picture of the relevant standardisation landscape.
  - ENISA: Overview of ICT certification laboratories, Jan 2018
  - ECSO: State of the Art Syllabus - Overview of existing Cybersecurity standards and certification schemes, Dec 2017) and

State of Play

- Proposal adopted in September 2017

- In negotiations with the co-legislators
  - Discussions on the proposal have begun in the Council
  - Draft reports published by IMCO and LIBE Committees of the European Parliament

- Goal: agreement before Q2 2019

Next steps –
With the European Cybersecurity Certification Framework in place

– "*Once the Framework is established, the Commission will invite the relevant stakeholders to focus on three priority areas*":

- Security in critical or high-risk applications.
- Cybersecurity in widely-deployed digital products, networks, systems and services such as email encryption, firewalls and Virtual Private Networks.
- "Security by Design" in low-cost, digital, interconnected mass consumer devices which make up the Internet of Things. For example:
  - Secure development methods including adequate security testing
  - Updates in the event of newly discovered vulnerabilities or threats.

- We are counting on your contribution.

Thank you for your attention!