EUROPEAN UNION AGENCY
FOR CYBERSECURITY

HOW TO TARGET CONTINUOUS COMPLIANCE?

STANDARDISATION AND CERTIFICATION IN THE EU

Sławomir Górniak
Senior Security Expert
Market, Certification and Standardisation Unit

25 | 11 | 2023

UNECE Disclaimer

The author and the speaker of this presentation confirm that they have authorization to use all photos and visual elements.

The material is either copyright-free or the author / speaker holds the necessary copyright.

The UNECE will remove any material from its events and supporting websites if there is unlawful use of copyrighted material.

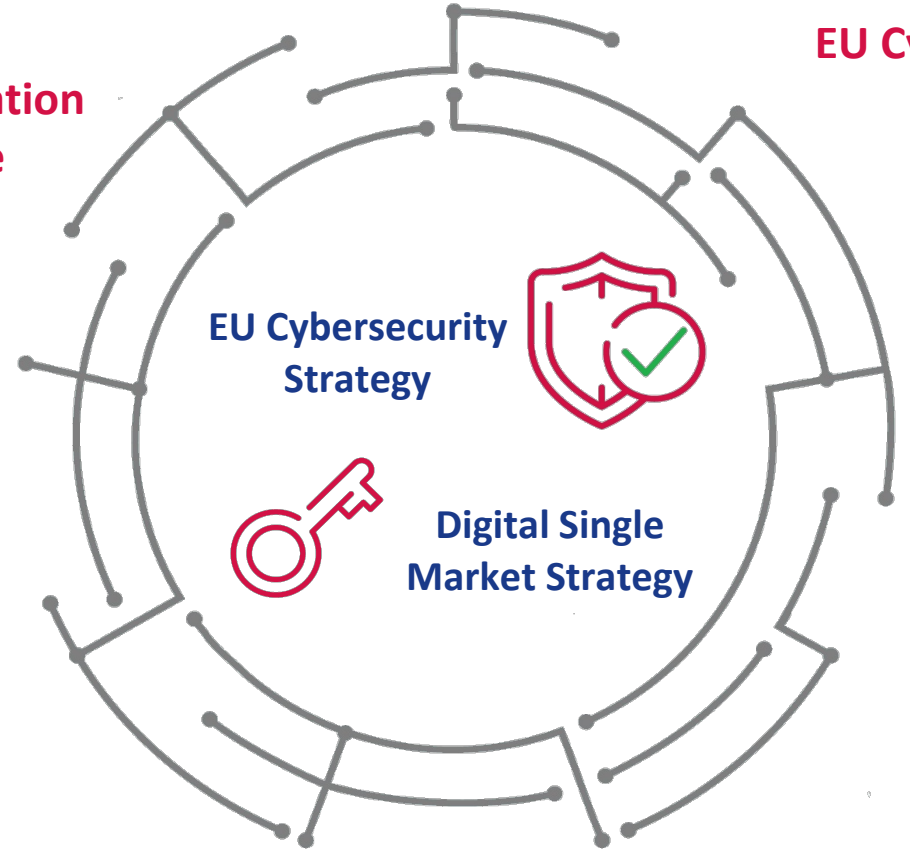
The author / speaker takes responsibility for any infringements on copyright and holds the UNECE harmless to this effect.

OPEN QUESTIONS

What could be considered as good cyber regulation with regard to continuous compliance?

How do you address changing product properties in products with embedded technologies?

EU LEGISLATION – CYBERSECURITY LANDSCAPE



Network and Information Security Directive

EU Cybersecurity Act

Radio Equipment Directive

General Data Protection Regulation

EU Chips Act

Cyber Resilience Act

eIDAS Regulation

Artificial Intelligence Act

Supply chain

EU Cyber Solidarity Act

Data Act

Digital Operational Resilience Act

Role of standards

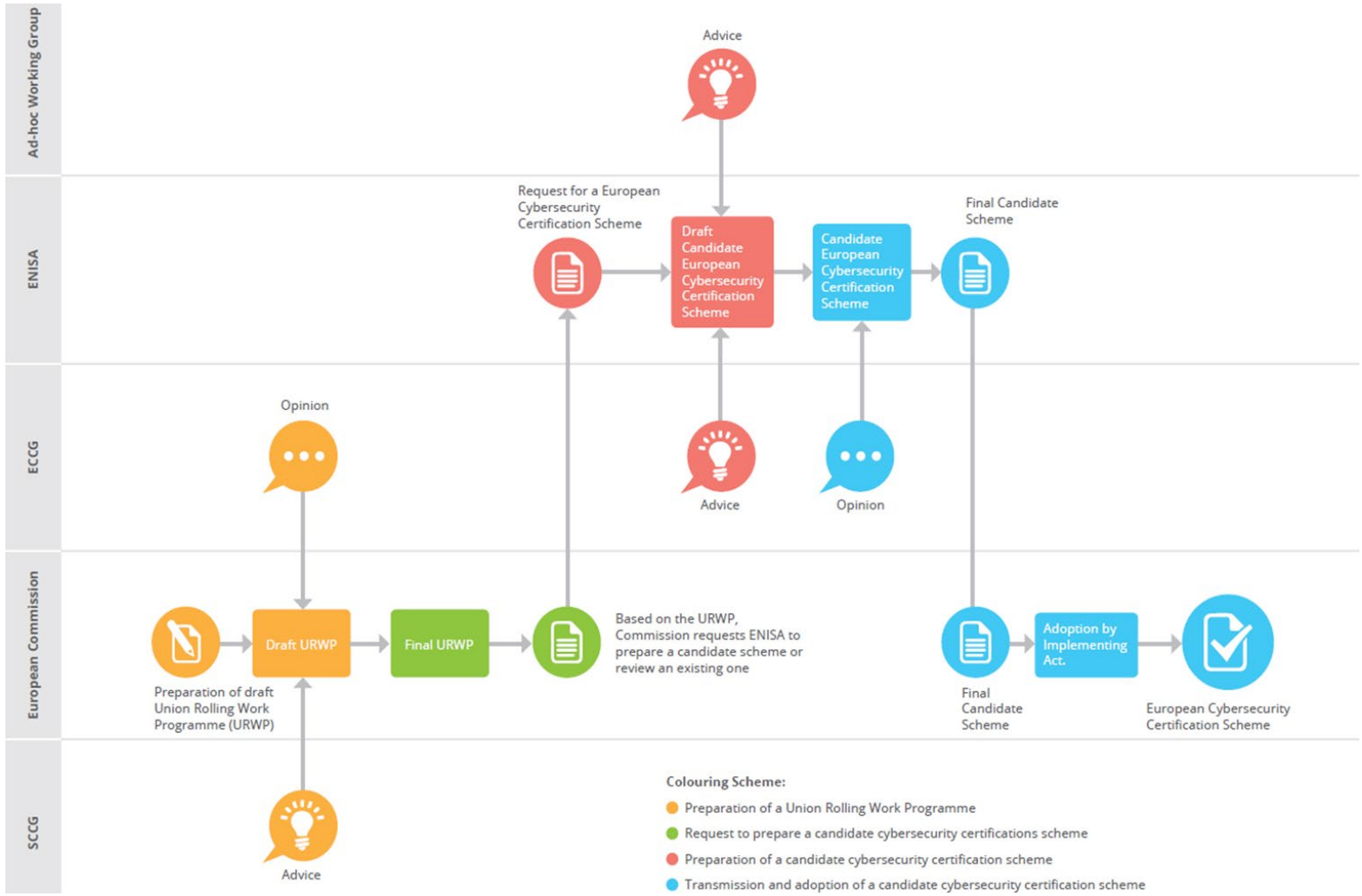
STANDARDISATION BODIES

EU CYBERSECURITY ACT

Standards

- **ENISA – the EU Agency for Cybersecurity**
  - Permanent mandate, strengthened tasks
  - Market related tasks, preparation of draft cybersecurity certification schemes, standardisation
  - Supporting the capacity building and preparedness across the Union
  - Support to the development of a coordinated response to large-scale cyber incidents and crises
  - Active support of the Commission and Member States with regard to the development and implementation of cybersecurity policy and legislation
- **Cybersecurity certification framework**
  - Addresses market fragmentation through a harmonized approach
  - Increase level of cybersecurity within the Union
  - A risk-based approach for voluntary certification covering cybersecurity of ICT products, services and processes
  - Adherence to Regulation (EU) 765/2008 on accreditation and market surveillance
  - Defined assurance levels (Basic, Substantial & High)
  - European cybersecurity certificates
  - European statements of conformity

EU CYBERSECURITY CERTIFICATION FRAMEWORK



EU CYBERSECURITY ACT – CERTIFICATION FRAMEWORK

- **EUCC: a horizontal ICT products scheme – comitology**
  - Common Criteria, ISO/IEC 17065 & 17025
  - Defines the “how to certify”, the “what to certify” is for risk owners to define through Protections Profiles
- **EUCS: a generic cloud services scheme**
  - Defines a baseline of requirements that are applicable to all services and enables the same methodology
  - **Specific standards under development**
- **EU5G: combining product security evaluation and product lifecycle processes evaluation**
  - As-is transposition of existing scheme elements - GSMA NESAS, SAS-SM Subscription Management, SAS-UP (UICC Production) and eUICC
  - Standards developed mainly by independent bodies
- **New requests for support**
  - EUDI Wallet
  - Cyber Resilience Act

CYBER RESILIENCE ACT – PROPOSAL (15 SEPTEMBER 2022)

"If everything is connected, everything can be hacked"

- **Impact assessment: no incentives to produce secure by design hardware and software**
- **Scope: Products with digital elements**
  - Hardware products and components placed on the market separately
  - Software products and components placed on the market separately
  - Also included remote data processing solutions
- **NOT covered:**
  - Non commercial projects, including open source
  - Services covered by NIS2, in particular cloud SaS
  - Certain products sufficiently regulated on cybersecurity

CYBER RESILIENCE ACT – PROPOSAL

- Cybersecurity rules for the placing on the market of hardware and software
- Obligations for manufacturers, distributors and importers
- Cybersecurity essential requirements across the life cycle (5 years)
- Conformity assessment differentiated by level of risk ('highly critical' – certification under CSA)
- Market surveillance and enforcement (prohibition, fines – up to 15M or 2,5% of turnover)
- **Harmonised standards** to follow
- Actions by ENISA – JRC – CEN-CENELEC – ETSI

THANK YOU FOR YOUR ATTENTION

Sławomir Górniak
Senior Cybersecurity Expert
Market, Certification and Standardisation Unit

European Union Agency for Cybersecurity

+30 697 00 151 63

slawomir.gorniak@enisa.europa.eu

www.enisa.europa.eu