

IN THE FRAMEWORK OF:

**SESEI**

Seconded European  
Standardisation  
Expert in India

Enabling Europe-India Cooperation on Standards



# 4<sup>th</sup> Indo-European Conference on Standards & Emerging Technologies

7th December 2023 | The LaLiT, New Delhi, India

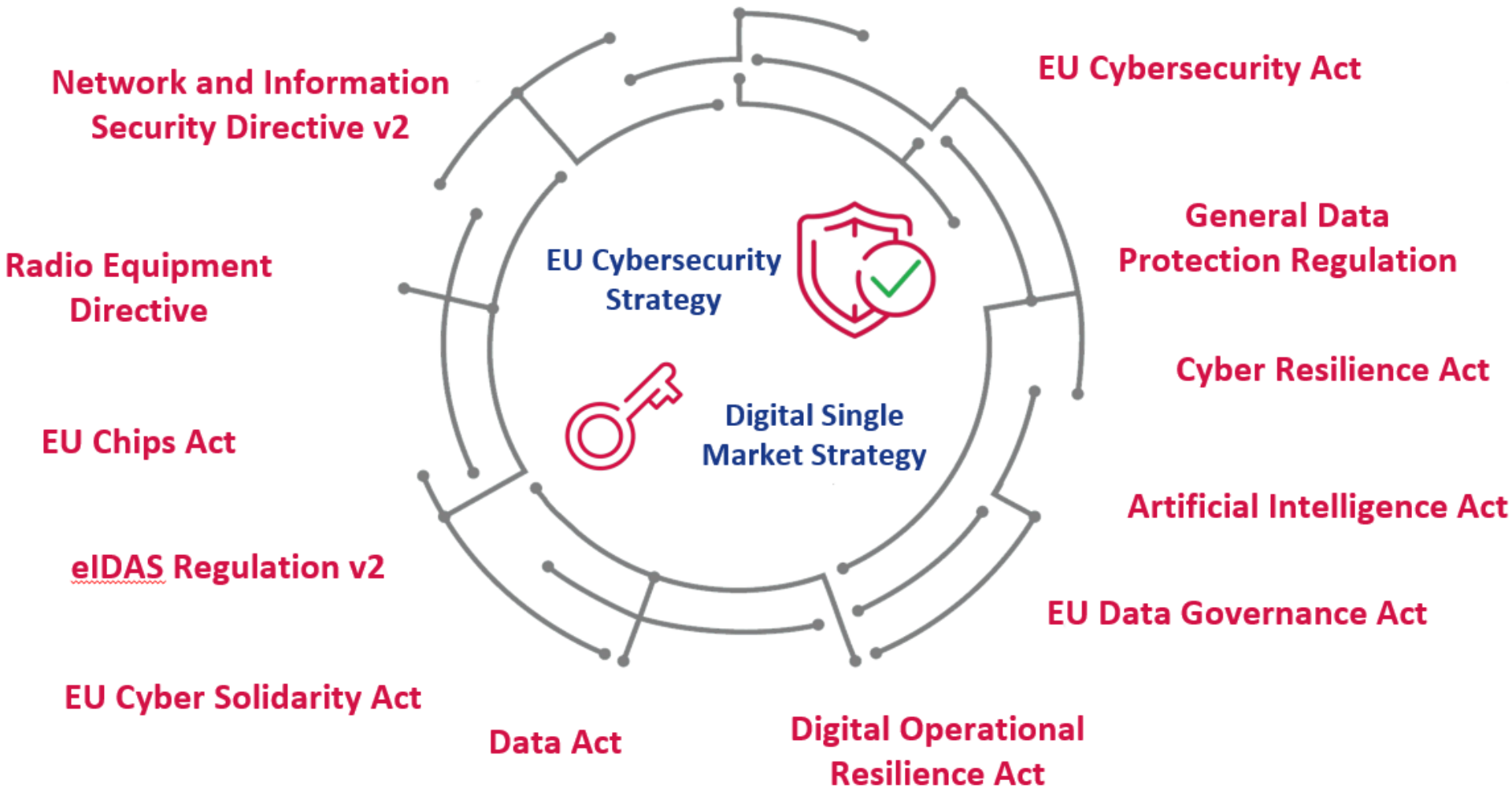
## EU CYBERSECURITY LEGISLATION & SUPPORT OF STANDARDISATION

**Sławomir Górniak**

**Senior Cybersecurity Expert**



# EU Legislation – Cybersecurity Landscape



# Standardisation Bodies



# EU Cybersecurity Act



- 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 Act – Certification Framework

- EUCC: a horizontal ICT products scheme – **commitology**
  - 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



# Network and Information Security Directive v2

Standards

- **New sectors** covered
- Stronger **risk and incident management** and cooperation
- Distinction between **essential and important** entities
- Size-cap rule
- Exclusion of micro and small enterprises, with exceptions indicated in the directive
- **Need for sectorial standards**



# eIDAS Regulation v2

Standards

- A **European Digital Identity Wallet** Framework
- **EU Toolbox** for a coordinated approach towards Digital Identity Framework
- **Certification** of “European Digital Identity Wallets” (art. 6) and of electronic identification schemes (art. 12) under the CSA
- Harmonised approach to trust, security and interoperability **through standards** (multiple articles)
- **New qualified trust services**
- Alignment of the Trust Service provisions with the rules applicable to **NISDv2** (articles 17, 18, 20, 21 and 24).
- **Issues:** standards for the EUDI Wallet interfaces, for Privacy Evaluation methodology, clear split of responsibility between the EU ESOs





# Cyber Resilience Act – proposal



*“If everything is connected, everything can be hacked”*

- 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





# Other EU legislation



- Radio Equipment Directive
  - Adopted in 2017, **Commission Delegated Regulation of 29/10/2021**
- Artificial Intelligence Act
  - Proposed 21 September 2021
- DORA Regulation (on digital operational resilience for the financial sector)
  - Proposed in 2020, **Published 27 December 2022**
- EU Cyber Solidarity Act
  - Proposed 18 April 2023
- European Data Act
  - Proposal – 23 February 2022, Political agreement 28 June 2023
- European Data Governance Act
  - Entered into force on 23 June 2022, applicable as of September 2023
- European Chips Act
  - Proposal – 8 February 2022, **Published 21 September 2023**






# THANK YOU FOR YOUR ATTENTION!

Sławomir Górnjak

Senior Cybersecurity Expert

Market, Certification and Standardisation Unit

European Union Agency for Cybersecurity

 +30 697 00 151 63

 [slawomir.gornjak@enisa.europa.eu](mailto:slawomir.gornjak@enisa.europa.eu)

 [www.enisa.europa.eu](http://www.enisa.europa.eu)

