EUROPEAN UNION AGENCY
FOR CYBERSECURITY

# STANDARDISATION AND CERTIFICATION – EU CHIPS ACT

Sławomir Górniak

Senior Security Expert

Market, Certification and Standardisation Unit

02 | 12 | 2022

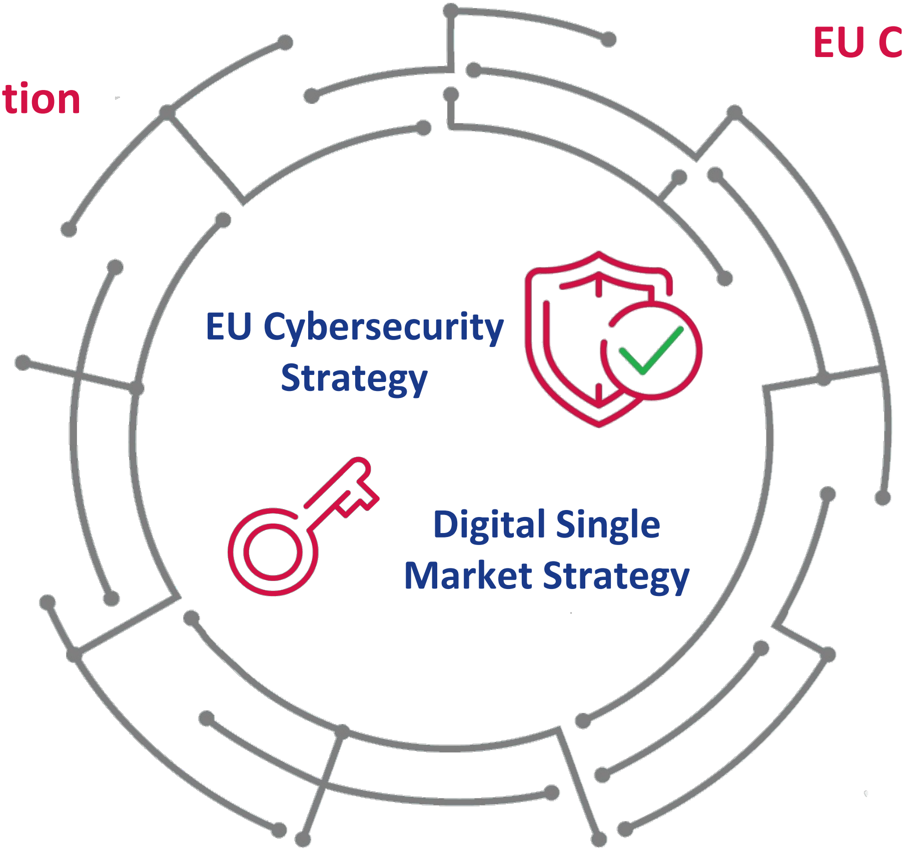
# EU LEGISLATION – CYBERSECURITY LANDSCAPE

Network and Information Security Directive

Radio Equipment Directive

EU Chips Act

eIDAS Regulation



EU Cybersecurity Strategy

Digital Single Market Strategy

EU Cybersecurity Act

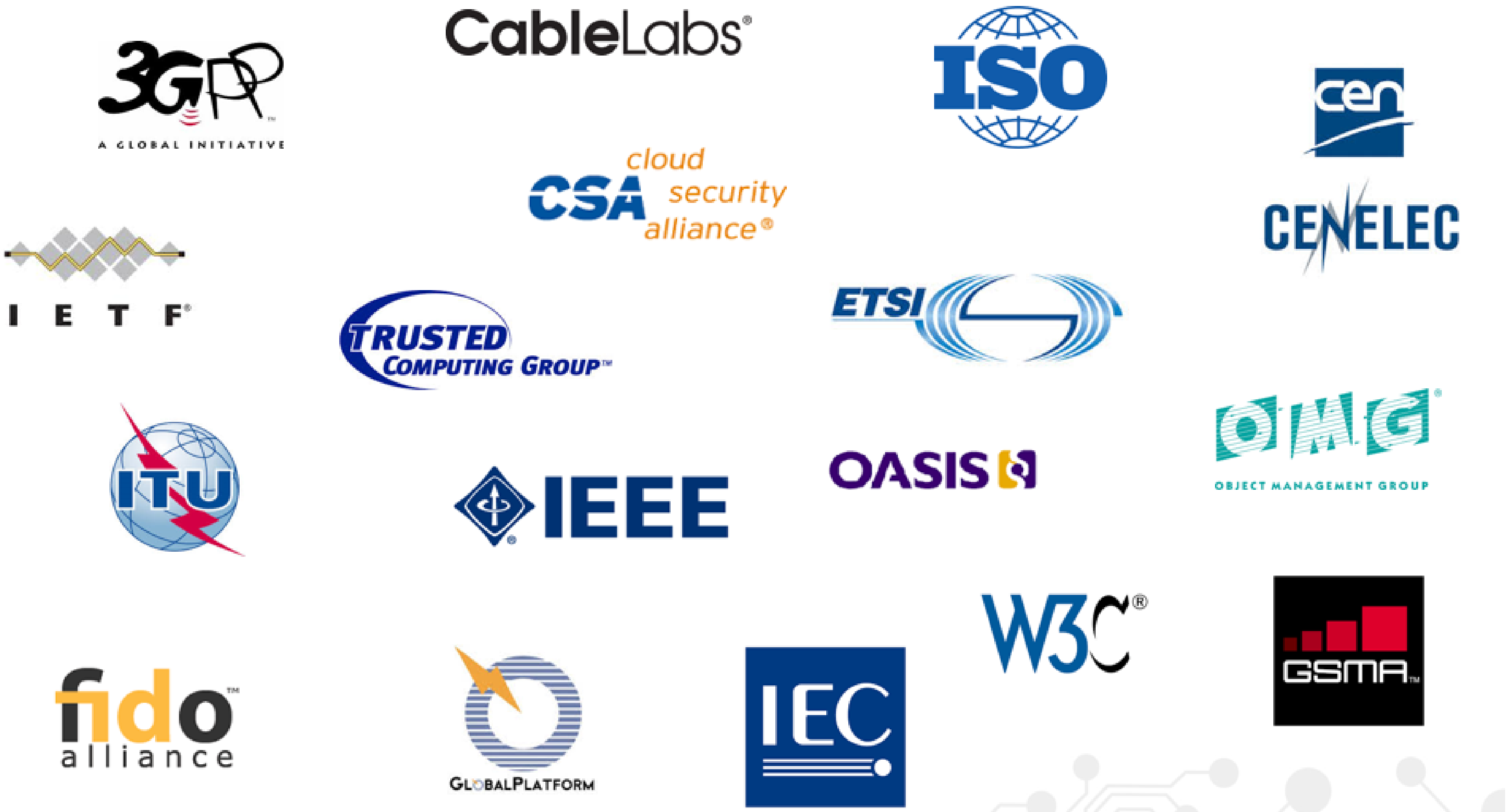
General Data Protection Regulation

Cyber Resilience Act

Artificial Intelligence Act

**Role of standards**

# STANDARDISATION BODIES



# EU CYBERSECURITY ACT – CERTIFICATION FRAMEWORK

- EUCC
  - Based on international standards – Common Criteria, ISO/IEC 17065 & 17025
- EUCS
  - Standards under development
    - CEN/CLC/JTC 13 /WG2: EUCS1 Security Objectives and Requirements for Cloud Services
    - CEN/CLC/JTC 13/WG3: EUCS2 Requirements for Conformity Assessment Bodies certifying Cloud Services
  - ISO/IEC 22123
- EU5G
  - “As-in” translation/Gap analysis of GSMA NESAS; GSMA SAS; GSMA SAS-UP and eUICC; focusing on 3GPP SA3
- CEN/CLC/JTC 13/WG3: Guidelines on sectoral cybersecurity assessment

# NISD V2 – UPDATES

- 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
- Art. 19 of eIDAS is repealed – inclusion of trust service providers in NIS2
- Art. 40 and 41 of Directive 2018/1972 establishing the European Electronic Communications Code are repealed
- **Need for sectorial standards**

# EIDAS V2 – UPDATES / PROPOSAL

- A European **Digital Identity Wallet** Framework
- The Recommendation for an **EU Toolbox** for a coordinated approach towards a European 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)
- Three **new qualified trust services** (provision of electronic archiving services, electronic ledgers and management of remote electronic signature and seal creation devices)
- Alignment of the Trust Service provisions with the rules applicable to **NIS2** (articles 17, 18, 20, 21 and 24).

# EIDAS V2 – STANDARDS

## Identified issues

- Lack of a clear legal definition of the term Digital Identity
- Need of the EU Mobile Application security and privacy evaluation methodology
- **Lack of standards for the EUDI Wallet interfaces** to QTSP, Relying Parties, Device, existing national eID documents (eID, E-pass, e-resident permit card, eDL) and existing eIDAS Nodes infrastructures
- **Lack of standards for a Privacy Evaluation methodology for general Digital Identity**
- Need for a clear split of responsibility between the EU ESO to avoid duplication
- No existing European standard for Mobile Application assessment methodology, creating some issue to reference applicable standards into the EU legislation

# AI ACT – ARTIFICIAL INTELLIGENCE / PROPOSAL

- AI Act content
  - Art 15 - Accuracy, robustness and cybersecurity
  - Art 42 – Presumption of conformity with certain requirements
- Aspects to consider
  - Integration of Cybersecurity in the risk assessment for the determination of high-risk systems
  - Necessary skills and competences of actors related to cybersecurity conformity assessment
  - Regulatory coherence with CSA
- EU Actions
  - Prepare for the adoption and implementation  of the AI Act (Art. 15)
  - Review of AI cybersecurity related standards
  - **Standardisation request to ESOs**

# AI ACT – STANDARDS

## Identified issues

- With specific guidance, general purpose standards can mitigate risks
- Still, a system-specific analysis is necessary as AI security objectives are often domain-specific
- Open debate: AI-specific horizontal standards vs vertical/sector specific
- Inherent features of ML not fully reflected in existing standards, esp. metrics and testing procedures
- Some areas not technologically mature enough to be standardized
- **No standards for organisations auditing, testing, certifying AI systems**

# CYBER RESILIENCE ACT – BASES

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

- 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, in particular cloud SaS, covered by NIS2
  - Certain products sufficiently regulated on cybersecurity
- **Harmonised standards to follow**
  - under evaluation: EC-JRC-ENISA

# OTHER LEGISLATIVE ACTS

- Radio Equipment Directive
    - Adopted in 2017
    - Commission Delegated Regulation of 29/10/2021
    - **Standardisation in progress**
- Future?

# SUPPLY CHAIN – OPPORTUNITIES FOR STANDARDISATION AND RESEARCH

- Improved and innovative trust models
- Evaluation and integrity checking techniques
- Solutions to detect and prevent counterfeiting / overproduction
- New approaches to security assurance
- Inventory/configuration control and maintenance
- Approaches for assessing policy needs on the global scale

# 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