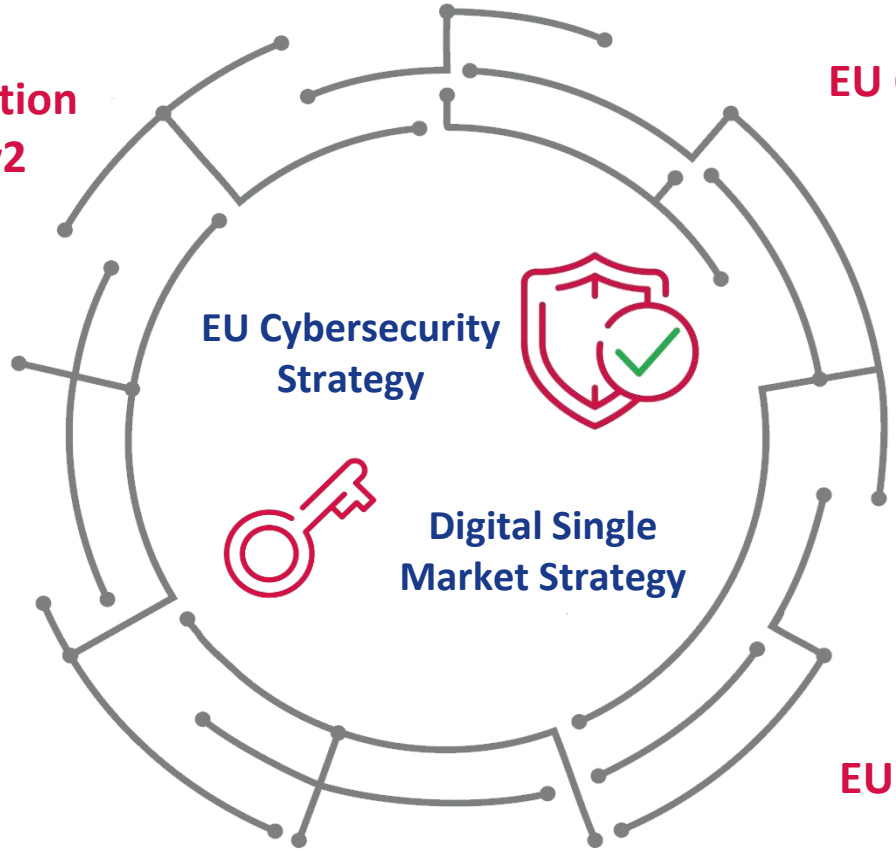
EUROPEAN UNION AGENCY
FOR CYBERSECURITY

EU CYBERSECURITY LEGISLATION & SUPPORT OF STANDARDISATION

Sławomir Górniak
Senior Security Expert
Market, Certification and Standardisation Unit

12 | 10 | 2023

EU LEGISLATION – CYBERSECURITY LANDSCAPE



Network and Information Security Directive v2

EU Cybersecurity Act

Radio Equipment Directive

General Data Protection Regulation

EU Chips Act

Cyber Resilience Act

eIDAS Regulation v2

Artificial Intelligence Act

EU Data Governance 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

NIS DIRECTIVE

Cloud Computing Services

Online Marketplaces

Search Engines

Strategic
Cooperation Network

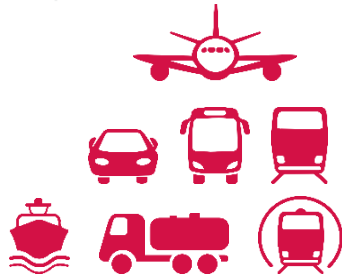
Digital Service Providers

Operators of Essential Services

Incident Reporting

Security Requirements

Tactical/Operational
CSIRT Network



Transport

National Cyber Security Strategies

Energy and Water

Healthcare

Banking and Financial market infrastructures

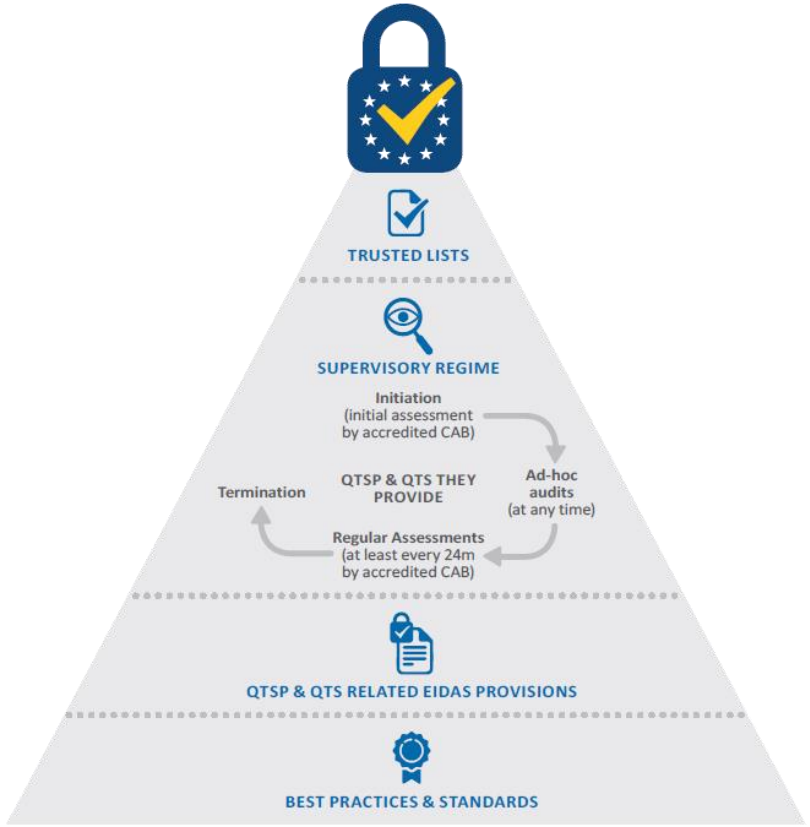
Digital Infrastructure

NISD V2 – UPDATES

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
- Art. 19 of eIDAS is repealed – inclusion of trust service providers in NISDv2
- Art. 40 and 41 of Directive 2018/1972 establishing the European Electronic Communications Code are repealed

EIDAS REGULATION – ELECTRONIC IDENTIFICATION AND TRUST SERVICES



EIDAS REGULATION V2 – UPDATES

Standards

- 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 **NISDv2** (articles 17, 18, 20, 21 and 24).

DIGITAL IDENTITY STANDARDS

ENISA study 2022 – major gaps in standardisation of EUDI Wallet

- No standards for the cryptographic device interface (direct interface of the cryptographic component of the mobile device;
- Functional testing requirements missing for elements of the EUDI Wallet except:
  - PID/(Q)EAA mutual authentication protocols,
  - qualified electronic signatures
- No standards fulfilling the EUDI Wallet needs in 100%
- All of the existing ones – designed for pure “on-line” or “off-line” use cases
- Draft ISO/IEC 23220 series (PID) designed to target the Digital Identity Wallet
- ETSI efforts
- Definition of the “What” and not the “How”
- Some use cases standardised

ARTIFICIAL INTELLIGENCE ACT – PROPOSAL

(21 SEPTEMBER 2021)

- **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**

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

EU CYBER SOLIDARITY ACT – PROPOSAL (18 APRIL 2023)

- Objectives
  - Strengthen common EU detection, situational awareness, and response capabilities
  - Gradually build an EU cybersecurity reserve with services from private providers
  - Support testing of critical entities.
- Implementation
  - Deployment of a pan-European infrastructure of Security Operations Centres (European Cyber Shield
  - Creation of a Cyber Emergency Mechanism to support MSs in preparing for, responding to and immediate recovery from significant and large-scale cybersecurity incidents
  - Establishment of a European Cybersecurity Incident Review Mechanism to review and assess specific significant or large-scale incidents.

OTHER EU LEGISLATION

- **Radio Equipment Directive**
  - Adopted in 2017
  - **Commission Delegated Regulation of 29/10/2021**
- **European Chips Act**
  - Proposal – 8 February 2022
  - **Published 21 September 2023**
- **DORA Regulation (on digital operational resilience for the financial sector)**
  - Proposed in 2020
  - **Published 27 December 2022**

OTHER EU LEGISLATION

- **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
  - Aim: facilitate data sharing across sectors and EU countries

OTHER INITIATIVES

- **European Cybersecurity Competence Centre**
  - Increase Europe’s cybersecurity capacities and competitiveness
  - Working together with a Network of National Coordination Centres (NCCs)
  - Building a strong cybersecurity Community
- **EU Cyber Diplomacy Toolbox**
  - Joint EU diplomatic response to malicious cyber activities
- **Cybersecurity Skills Academy**
  - Single point of entry for cybersecurity education& training offers and funding opportunities (virtual platform)

CERTIFICATION SCHEMES – UPDATE

- **EUCC: a horizontal ICT products scheme – under consultations!**
  - 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.
  - Enables the same methodology for all services
  - Does not assess the security of product-specific security features (Security as a Service)
  - 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
  - Development of the candidate scheme
  - Standards developed mainly by independent bodies

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