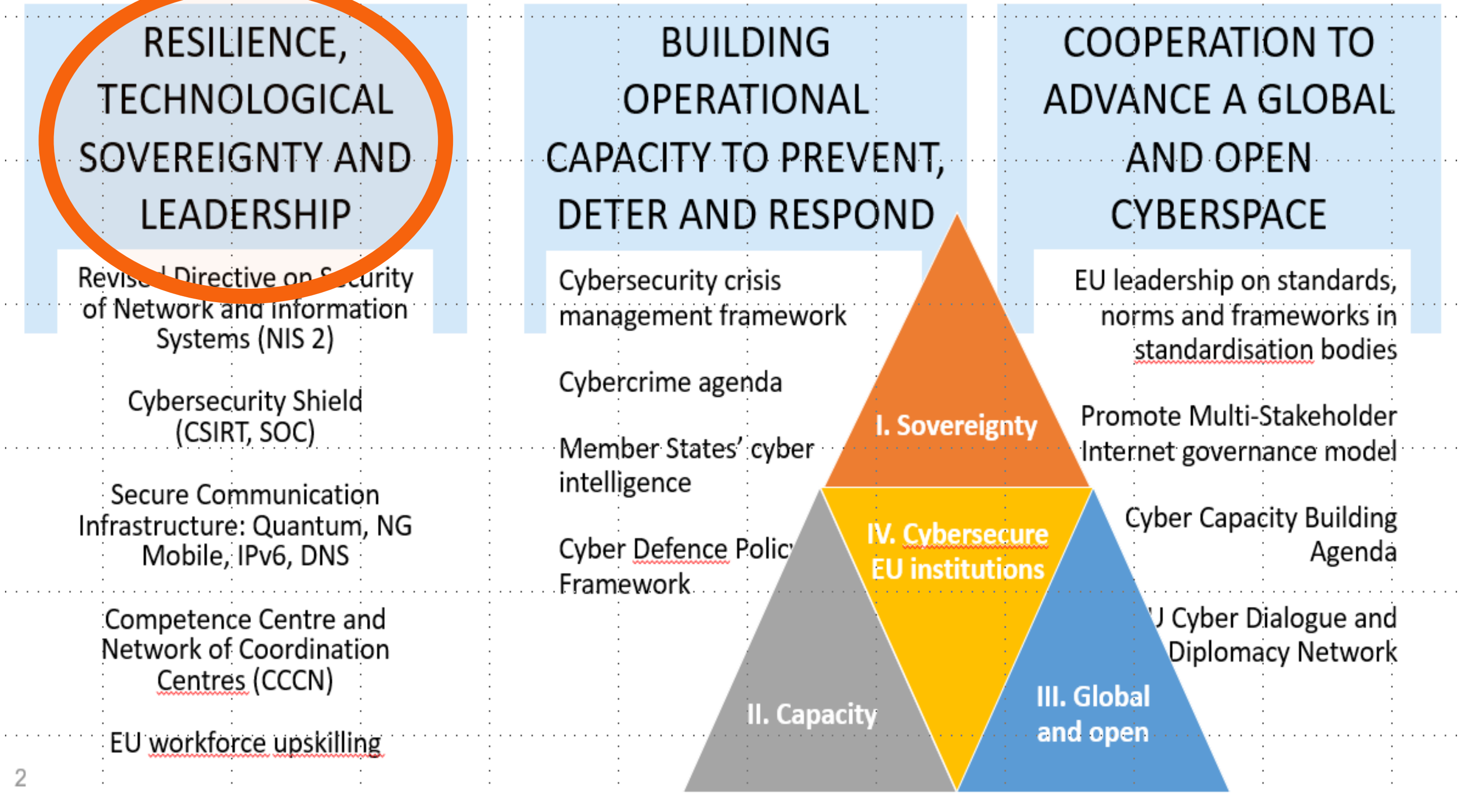
EU Cybersecurity Law Overview – The Policy Context

The **Digital Single Market Strategy** is built around improving access to goods, services and content, creating the appropriate legal framework for digital networks and services, and reaping the benefits of a data-based economy. A European Digital Single Market needs security and trust on behalf of the consumers; there is in need of a **homogeneous interpretation of the rules for Cybersecurity**, including mutual recognition between Member States.

A policy tool, the revised **EU Cybersecurity Strategy** has been launched in 2020 to replace the outdated 2013 communication, as to provide a framework and objectives of Commission's plans. The Strategy supports **the Digital Decade 2030 Strategy objective for secure digital transformation.**



RESILIENCE, TECHNOLOGICAL SOVEREIGNTY AND LEADERSHIP

- Revised Directive on Security of Network and Information Systems (NIS 2)
- Cybersecurity Shield (CSIRT, SOC)
- Secure Communication Infrastructure: Quantum, NG Mobile, IPv6, DNS
- Competence Centre and Network of Coordination Centres (CCCN)
- EU workforce upskilling

BUILDING OPERATIONAL CAPACITY TO PREVENT, DETER AND RESPOND

- Cybersecurity crisis management framework
- Cybercrime agenda
- Member States' cyber intelligence
- Cyber Defence Policy Framework

COOPERATION TO ADVANCE A GLOBAL AND OPEN CYBERSPACE

- EU leadership on standards, norms and frameworks in standardisation bodies
- Promote Multi-Stakeholder Internet governance model
- Cyber Capacity Building Agenda
- EU Cyber Dialogue and Diplomacy Network

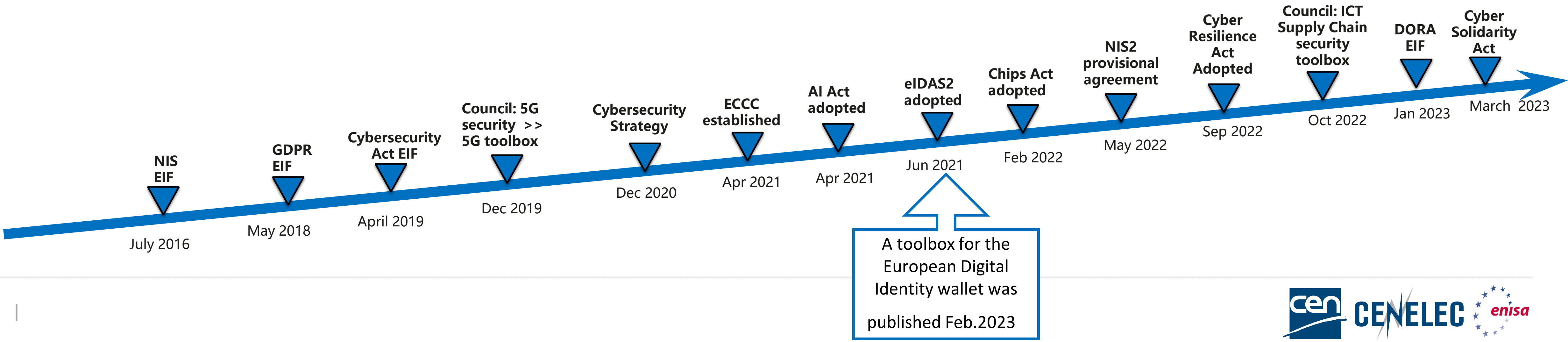
The EU's resilience and technological sovereignty needs to be founded on the resilience of all connected services and products, as to enable a secure digital transformation

During the last 5 years we have observed cataclysmic developments in the policy and law terrain.

A number of legislative tools (new or revisions) with direct or indirect relation to cybersecurity have been adopted and more are to be expected in the following year/s: **The Cybersecurity Act CSA), Radio Equipment Directive (DA), General Data Protection Regulation (GDPR), Digital Operational Resilience Act (DORA), Network and Information Security Directive (NIS2),**

as well as a number of proposed legislation, such as, **European Chips Regulation (The Chips Act), Artificial Intelligence Act (AIA), EU regulation on electronic identification and trust services for electronic transactions (eIDAS2), the Cyber Resilience Act (CRA**) and the expected **Cyber Solidarity Act…**

…are all pieces of the puzzle of the cybersecurity strategy to build a cybersecurity protection umbrella for businesses, citizens and state actors.



NIS EIF July 2016

GDPR EIF May 2018

Cybersecurity Act EIF April 2019

Council: 5G security >> 5G toolbox Dec 2019

Cybersecurity Strategy Dec 2020

ECCC established Apr 2021

AI Act adopted Apr 2021

eIDAS2 adopted Jun 2021

A toolbox for the European Digital Identity wallet was published Feb.2023

Chips Act adopted Feb 2022

NIS2 provisional agreement May 2022

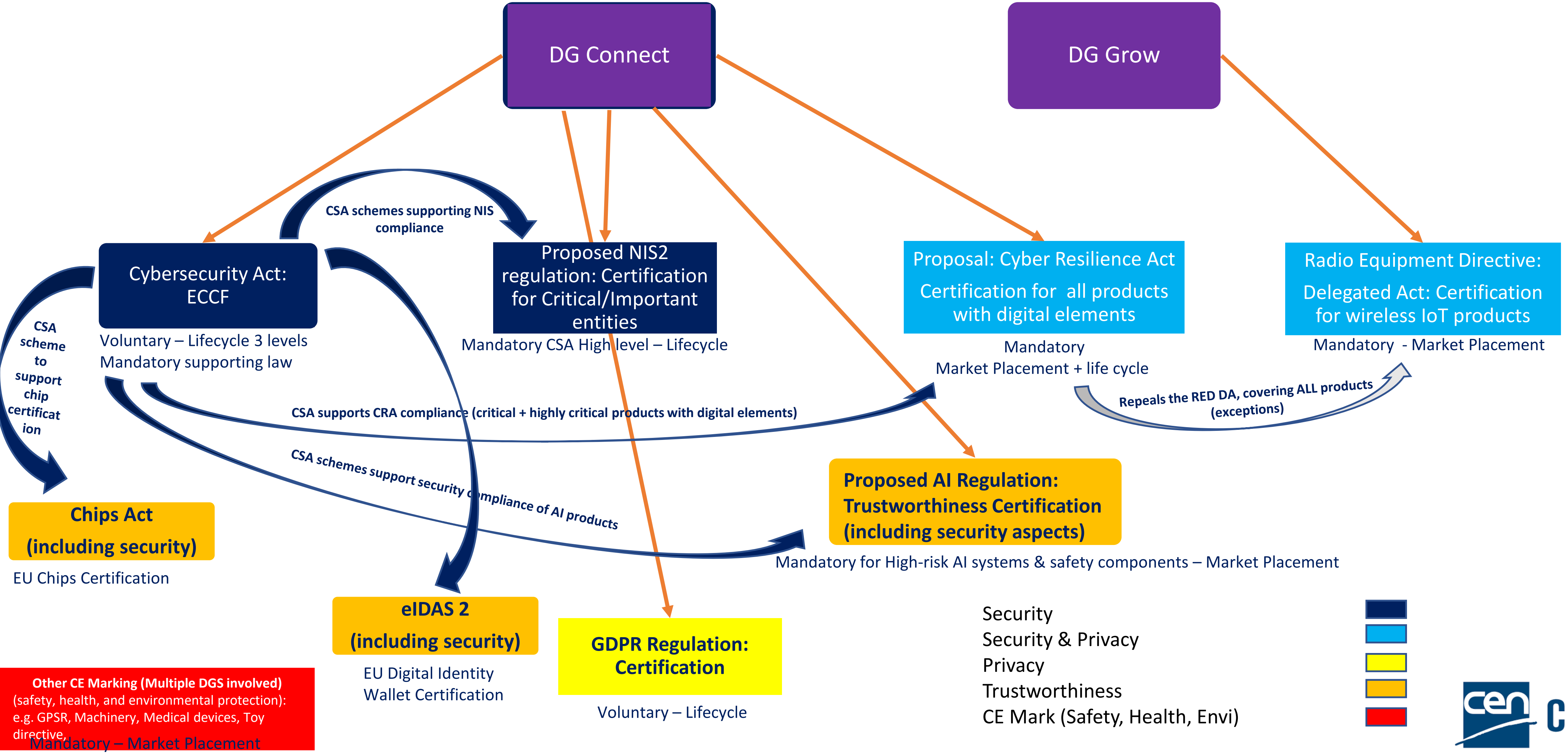
Cyber Resilience Act Adopted Sep 2022

Council: ICT Supply Chain security toolbox Oct 2022

DORA EIF Jan 2023

Cyber Solidarity Act March 2023

EU Cybersecurity Law Interplay (Conformity Assesssment View)



DG Connect

DG Grow

Cybersecurity Act: ECCF

Voluntary – Lifecycle 3 levels
Mandatory supporting law

Proposed NIS2 regulation: Certification for Critical/Important entities

Mandatory CSA High level – Lifecycle

Proposal: Cyber Resilience Act

Certification for all products with digital elements

Mandatory
Market Placement + life cycle

Radio Equipment Directive:

Delegated Act: Certification for wireless IoT products

Mandatory - Market Placement

CSA schemes supporting NIS compliance

CSA scheme to support chip certification

CSA supports CRA compliance (critical + highly critical products with digital elements)

Repeals the RED DA, covering ALL products (exceptions)

CSA schemes support security compliance of AI products

Chips Act (including security)

EU Chips Certification

Proposed AI Regulation: Trustworthiness Certification (including security aspects)

Mandatory for High-risk AI systems & safety components – Market Placement

eIDAS 2 (including security)

EU Digital Identity Wallet Certification

GDPR Regulation: Certification

Voluntary – Lifecycle

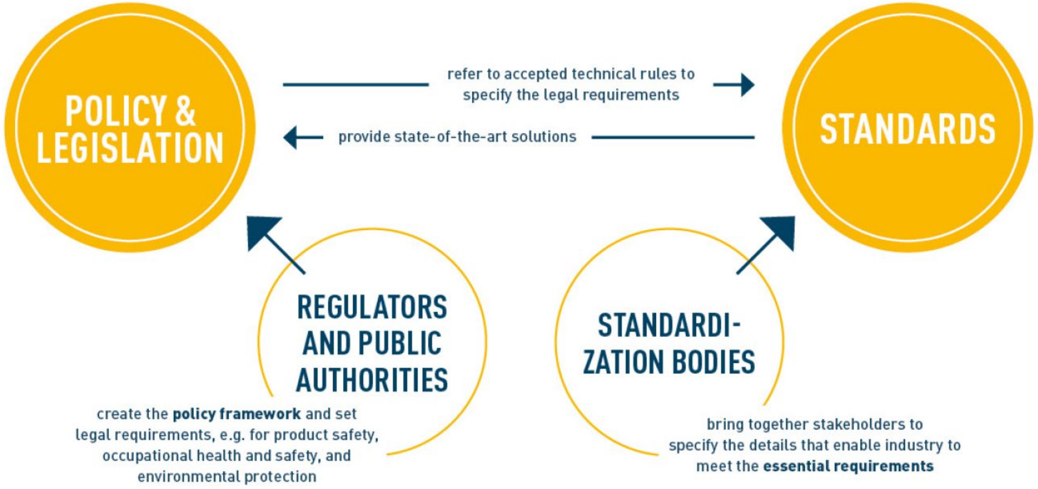
Other CE Marking (Multiple DGS involved) (safety, health, and environmental protection): e.g. GPSR, Machinery, Medical devices, Toy directive,

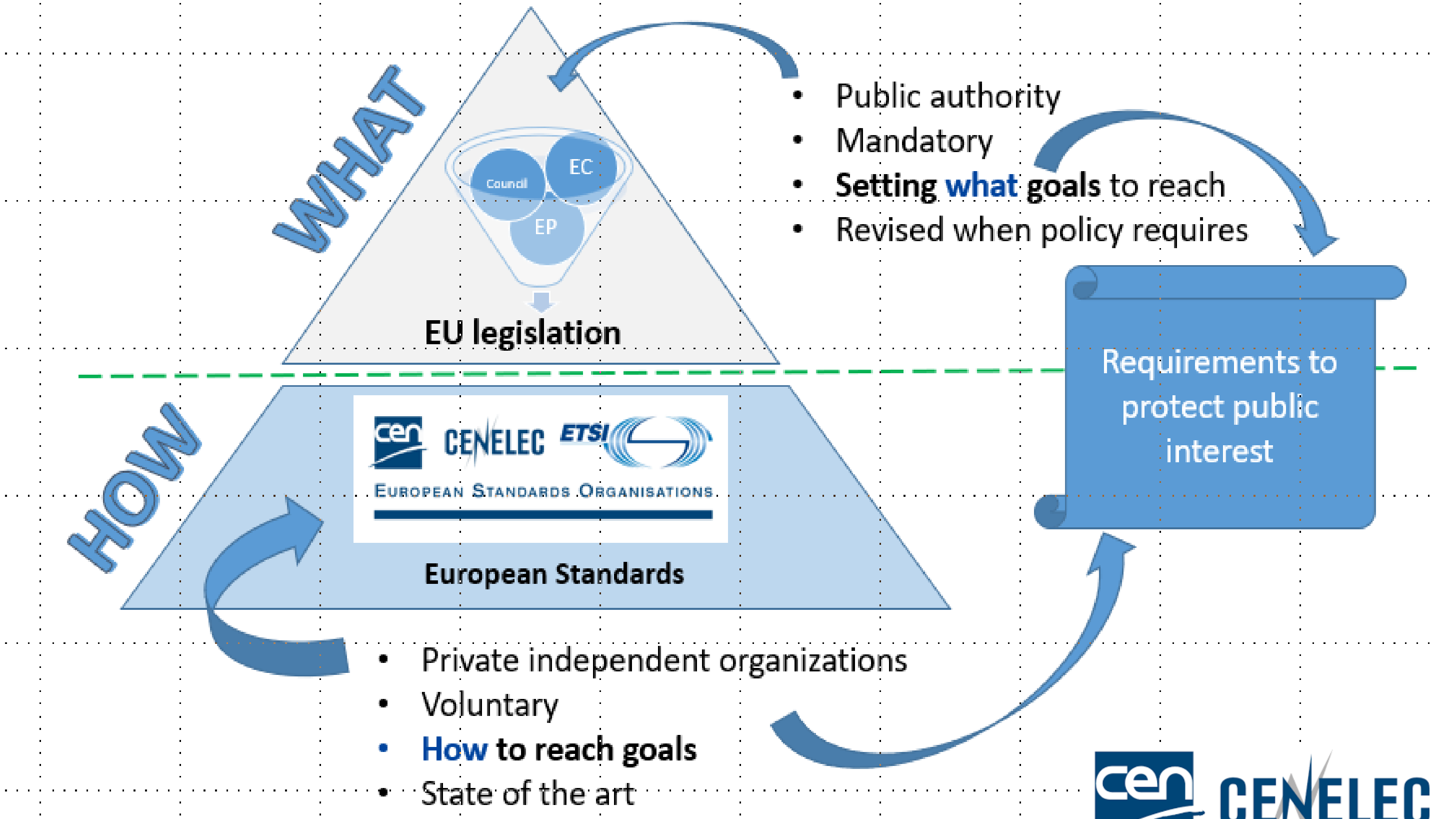
Mandatory – Market Placement

Security	■
Security & Privacy	🟦
Privacy	🟨
Trustworthiness	🟧
CE Mark (Safety, Health, Envi)	🟥

EU Cybersecurity Law Overview – Standardisation and NLF

- A **certification framework and certification schemes and processes for the different sectors could/should provide a common baseline**.
- However, different approaches must be provided for different sectors due to the way they function. It is important to stress, that diverse approaches must **align on one important common denominator; to follow the new legal framework process, widely known as NLF**. **CEN and CENELEC** have stressed in numerous occasions, the importance of the NLF for the development of standards and standardization infrastructure within the European Single Market.
- At the core of the **NLF is the practice of the 'presumption of conformity', meaning that by using a harmonised standard, a manufacturer is deemed to comply with the requirements of regulation**.


POLICY & LEGISLATION
refer to accepted technical rules to specify the legal requirements
provide state-of-the-art solutions
STANDARDS
REGULATORS AND PUBLIC AUTHORITIES
create the policy framework and set legal requirements, e.g. for product safety, occupational health and safety, and environmental protection
STANDARDI-ZATION BODIES
bring together stakeholders to specify the details that enable industry to meet the essential requirements


WHAT
Council
EC
EP
EU legislation
Public authority
Mandatory
Setting what goals to reach
Revised when policy requires
Requirements to protect public interest
HOW
cen
CENELEC
ETSI
European Standards Organisations
European Standards
Private independent organizations
Voluntary
How to reach goals
State of the art

CEN CENELEC SUPPORTING CYBERSECURITY LAW AND EU SCHEMES

- In the meantime, the **Cybersecurity Act is now at full speed**. Three schemes have already been requested by the Commission, and three AHWGs have been respectively established by ENISA to develop cybersecurity certification schemes (**EUCC, EUCS, EU5G**).

- **CEN CENELEC JTC13 is in the process of adapting to policy and legal developments t**hat create new challenges and opportunities for its involvement, as to support cybersecurity initiatives and legislation adopted by the Commission and cybersecurity schemes launched by ENISA. To this end JTC13, is developing standards to support the EUCS and soon will be involved in EU5G.

- For the first time ever JTC13 is now developing harmonized standards to support the implementation of the Radio Equipment Directive DA {articles 3(3) d,e,f} – essentially the first law that provides mandatory baseline cybersecurity requirements for market placement if wireless IoT products.

EUCS – CLOUD SERVICES SCHEME

EUCS, a candidate cybersecurity certification scheme for cloud services

DECEMBER 2020

EU CYBERSECURITY CERTIFICATION FOR 5G NETWORKS

enisa

EUROPEAN UNION AGENCY FOR CYBERSECURITY

CYBERSECURITY CERTIFICATION

EUCC, a candidate cybersecurity certification scheme to serve as a successor to the existing SOG-IS

enisa

CEN CENELEC

Thank You