TRUST
IN
DIGITAL
LIFE

POLICY TOOLS FOR TRUST:
STANDARDS AND CERTIFICATIONS FOR AI AND CYBERSECURITY

A TDL Roundtable
14:30-16:30 14 November 2023
Digital Europe, rue de la Science 37, Brussels

THE ROUNDTABLE

The overall theme of the roundtable was certification, standardisation and trust challenges:

- *firstly, to address operational aspects related to the implementation of the Cyber Resilience Act; and*
- *secondly, to broaden the scope to include 5G, AI, cloud and technology more broadly.*

The driver was the impact on hardware and software development and ultimately users, and TO raise questions relating to conformity assessments, their cost to manufacturers particularly in the absence of adequate, relevant standards.

- *Are standards and certifications the silver bullet for trust?*
- *What is their added value to build global trust?*
- *What are the limits and potential bottlenecks down the road?*

These compelling issues – and more – were discussed with a selected group of experts from academia and industry as well as standardisation and certification bodies.

The discussion was facilitated by short presentations and then the floor was opened to all participants for input and reactions (Chatham House rules i.e., non-attribution of sources).

CONTENTS

Issues

Keynote: Upcoming European regulations on AI and Cybersecurity

Keynote: Building trust with standards

Discussion

Priorities

ISSUES

(1) Are standards and certifications the silver bullet for trust?

- What is their added value to build global trust?
- What are the limits and potential bottlenecks down the road?

(2) To what extant do these tools build trust on top of compliance?

- High level of transparency, security - how can customers assess?
- How do we decide different trust levels beyond compliance?

(3) As a global company, can we assume that EU legal compliance is most trusted?

- But is this enough in all markets or is there something else needed, locally and globally?

ISSUES

(4) How is trust impacted by lack of skills?

- Is there a role for academia?

(5) Standards / certifications were originally meant to measure 'things': what are the measurable aspects of trust?

- Are applying European values in standards relevant? How do we build standards based on European values?

ISSUES

(6) Should there be a broader society representation in creating standards?

- What is the role of industry in non-measurable criteria, is there a role for other stakeholders
- Should non-European companies with expertise, who are currently excluded because of European values, be involved?
- Should values and trust be prioritised to the exclusion of expertise? Can standards – being based on values – be built without technical expertise of industry?

Upcoming European regulations on AI and Cybersecurity

Selected recent European regulation initiatives

Europe

- We focus on 4 key European pillars developing guidance on Cybersecurity, Privacy and AI. Some introduce on device „essential requirements“ which need to be met for access to single European Market. Further items: Draft EU Data Act published Feb‘22 [5], General Data Protection Regulation [6], NIS 2.0 (published, in implmentation) etc.

Draft AI Regulation [1]
(Essential Requirements for Market Access)

Under control of EC, Directorate General CNECT

Radio Equipment Directive (RED) [2]
(Essential Requirements for Market Access)

Under control of EC, Directorate General GROW

Draft Cyber Resilience Act (CRA) [3]
(Essential Cyber Requirements for Market Access for all Connected Products)

Under control of EC, Directorate General CNECT

Cybersecurity Act [4]
(Introduces 3 levels of cybersecurity: basic, substantial, high)

schemes prepared by ENISA upon EC request and then adopted by EC

Introduce essential requirements
(High-Risk AI / Radio Systems / Products with digital elements/ All connected products (CRA))

(voluntary) certification schemes, may become mandatory

Timelines (Expected)

RED

Regulation	Stand. Req	Stand. Dev
☑	☑	ongoing

The obligations related to new RED Articles will be applicable as of 1 August 2025 (from 2024). Standardization Request to CEN/CENELEC.

Cyber Resilience Act

Regulation	Stand. Req	Stand. Dev
Draft ☑	Draft ☑	TBC

Draft regulation & 1st draft Standardization Request available. Entry into force ~2025 (Art. 11 CRA), ~2026 (full CRA).

AI Regulation

Regulation	Stand. Req	Stand. Dev
Draft ☑	☑	TBC

Draft regulation & 1st draft Standardization Request available. Publication in OJEU expected early 2024, entry into force ~2026.

DISCUSSION

There are a plethora of regulations for industry and a brief implementation period which is a big challenge

Typically, there are three stages:

1. A regulation from the Institutions
2. ETSI / CEN / CENELEC involvement
3. Harmonised European norms such as types of features, how to test

There is the minimum level of acceptance in order to pass compliance, but this is not good to meet trustworthiness OR customer expectations

What goes beyond the strict requirements for market access?

Also moving from the physical to functional – how is it possible to assess whether a manufacturer is meeting a functional requirement?

A game changer for industry is managing compliance over a product lifetime.

What are the real challenges of introducing European values into standards

DISCUSSION

What are the real challenges of introducing European values into standards?

Europe started to incorporate European values with the AI Act, but balancing technical requirements with values is a significant challenge.

Policy tools for trust: Standards and certifications for AI and cybersecurity

European AI Act
Overview of technical standardisation

Contents

- Building trust with standards
- How EU shapes standardisation
    - Research & innovation shaping
    - Direct standardisation request
- AI Act impact on business scenario

Standards : Silver bullet for creating trust?

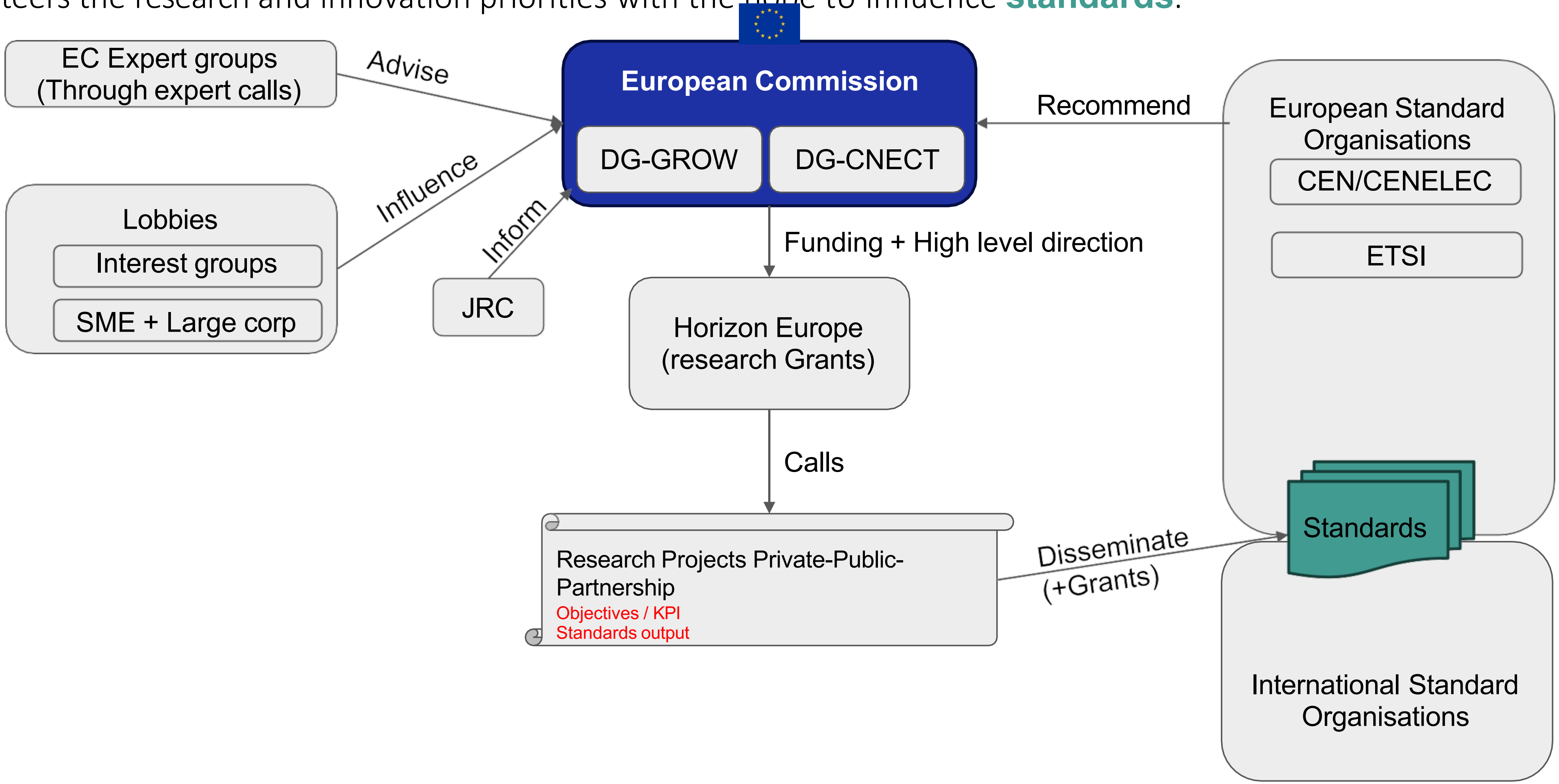
- Standards only bring trust if they are being used !
- Two traditional ways standards are used to build trust :
  - Voluntary adoption by the industry (benefit of interoperability, creating a bigger cake)
    - Common tools / framework / Industry specifications
  - Mandatory Certification/ Conformance / Audit
    - Harmonised standards / Trusted laboratory
- Standard can build trust with :
  - Clear definitions
  - Implementation management system
  - Documenting systems
  - Checks of functional requirements
  - Established testing methodologies for explaining and reporting

Standards : Silver bullet for creating trust?

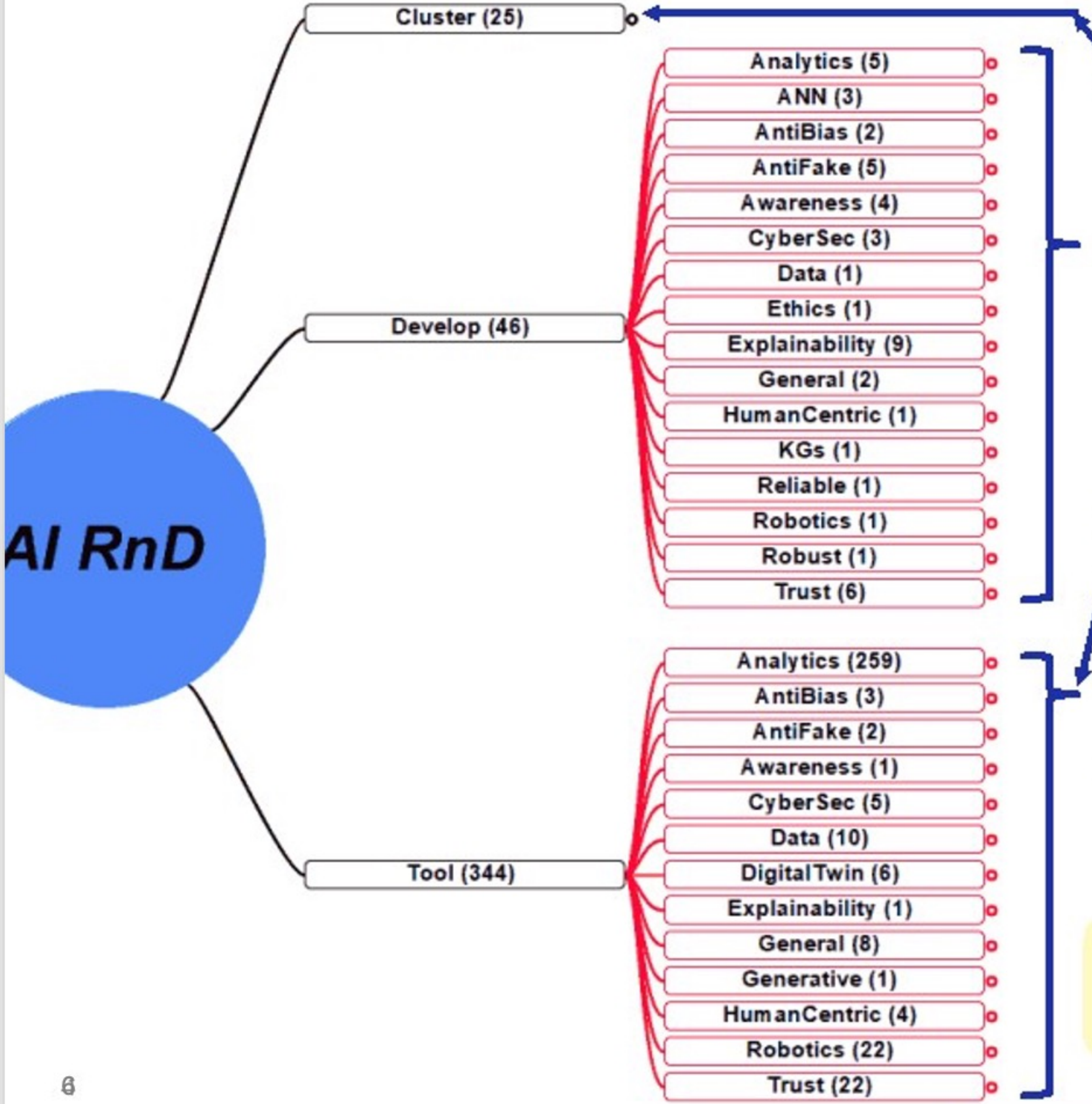
- Challenges in building trust with standards
  - Difficulty to access the standard (need to pay for standards)
  - Standard obsolete, late to market
  - Standard not fit for purpose
    - Difficult to understand / implement
    - Lack of tools
    - Lack of experts
    - Lack of required features in products for compliance
  - Standard not clear enough, room for different interpretation
  - Standard not specifying testing methodology (Pass/Fail Criteria)
  - Multiple competing standards (betting on the right horse)

Europe funding : Research/innovation & standardisation

Europe steers the research and innovation priorities with the hope to influence **standards**.



EC Research Investments : over 400 ongoing projects for AI



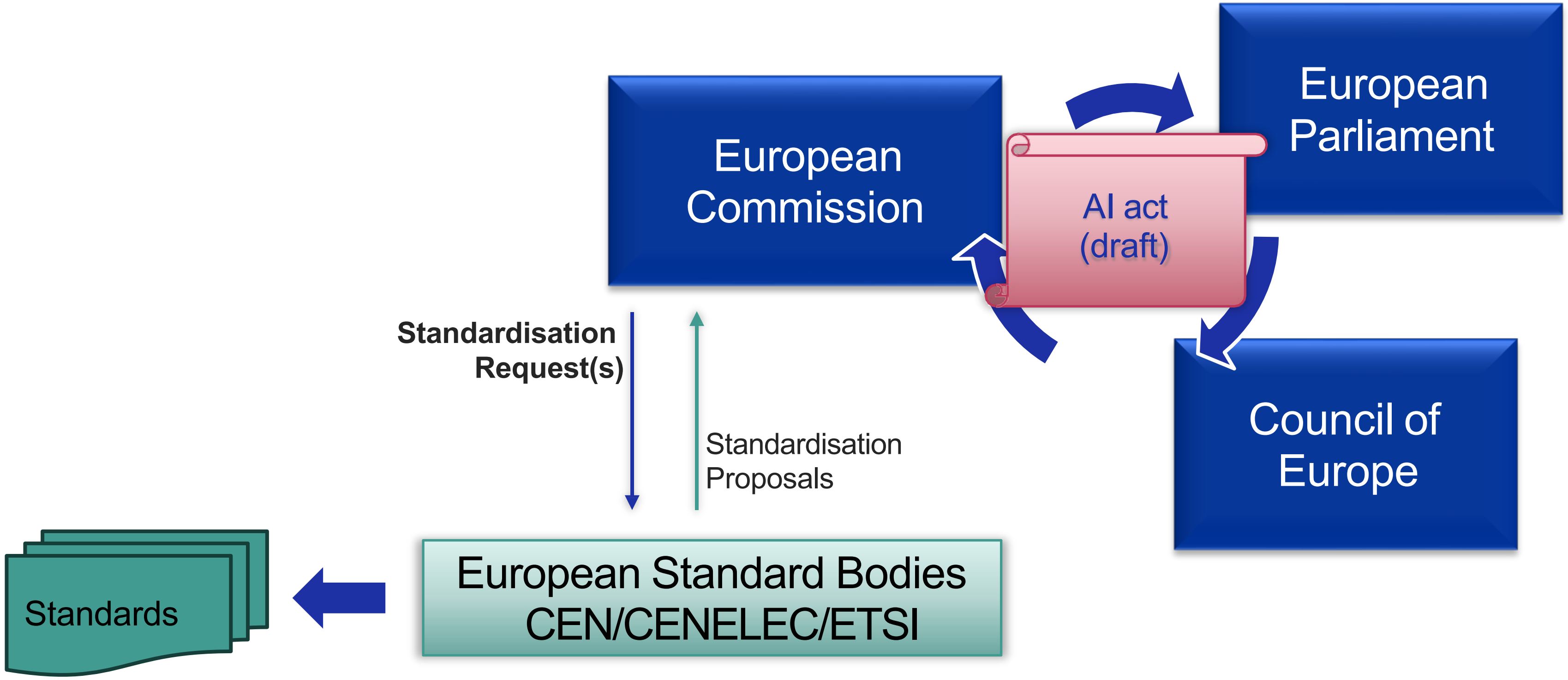
AI RnD

- Cluster (25)
- Develop (46)
  - Analytics (5)
  - ANN (3)
  - AntiBias (2)
  - AntiFake (5)
  - Awareness (4)
  - CyberSec (3)
  - Data (1)
  - Ethics (1)
  - Explainability (9)
  - General (2)
  - HumanCentric (1)
  - KGs (1)
  - Reliable (1)
  - Robotics (1)
  - Robust (1)
  - Trust (6)
- Tool (344)
  - Analytics (259)
  - AntiBias (3)
  - AntiFake (2)
  - Awareness (1)
  - CyberSec (5)
  - Data (10)
  - DigitalTwin (6)
  - Explainability (1)
  - General (8)
  - Generative (1)
  - HumanCentric (4)
  - Robotics (22)
  - Trust (22)

- 25 projects fund groups of universities and industry partners to collaborate (cluster)
- 46 projects aim to _improve_ AI in topics like explainability (9), trust (6), cybersec (3)
- 344 projects _use_ AI as a tool for data analytics (259) or robotics (22)
  <u>or also topics relevant to AI ACT</u>: detecting bias (3), detecting fakes (2), trust (22)
- >100 projects develop/use AI for Health

- many research projects relate to AI ACT
  ➔ many "gaps" standards cannot yet fill

EU standardisation : Harmonised standards



- The EC has selected CEN/CENELEC to answer the **Standardisation Request** to provide standards to support the AI Act.
- The EC issued the standardisation to CEN/CENELEC request in May 2023, provided it collaborated with ETSI.

Standardisation request (22/05/2023) - C(2023)3215 (europa.eu)

Reminder : Types of standards

- What are we standardising ? - Foundational and terminology standards for AI

Set up key concepts and terminology for artificial intelligence (AI). Baseline for the development of other standards for AI and to support communication between diverse stakeholders developing or impacted by AI.

- How should we develop it ? - Process and management standards for AI

Define organizational processes and approaches. Process and management standards are being adapted for the AI context to set out repeatable guidance, for example for risk management processes or transparency reporting.

- Is it working as it should ? - Performance requirements for AI

Product testing and performance standards are being used to benchmark AI system performance and set out requirements for robustness and security.

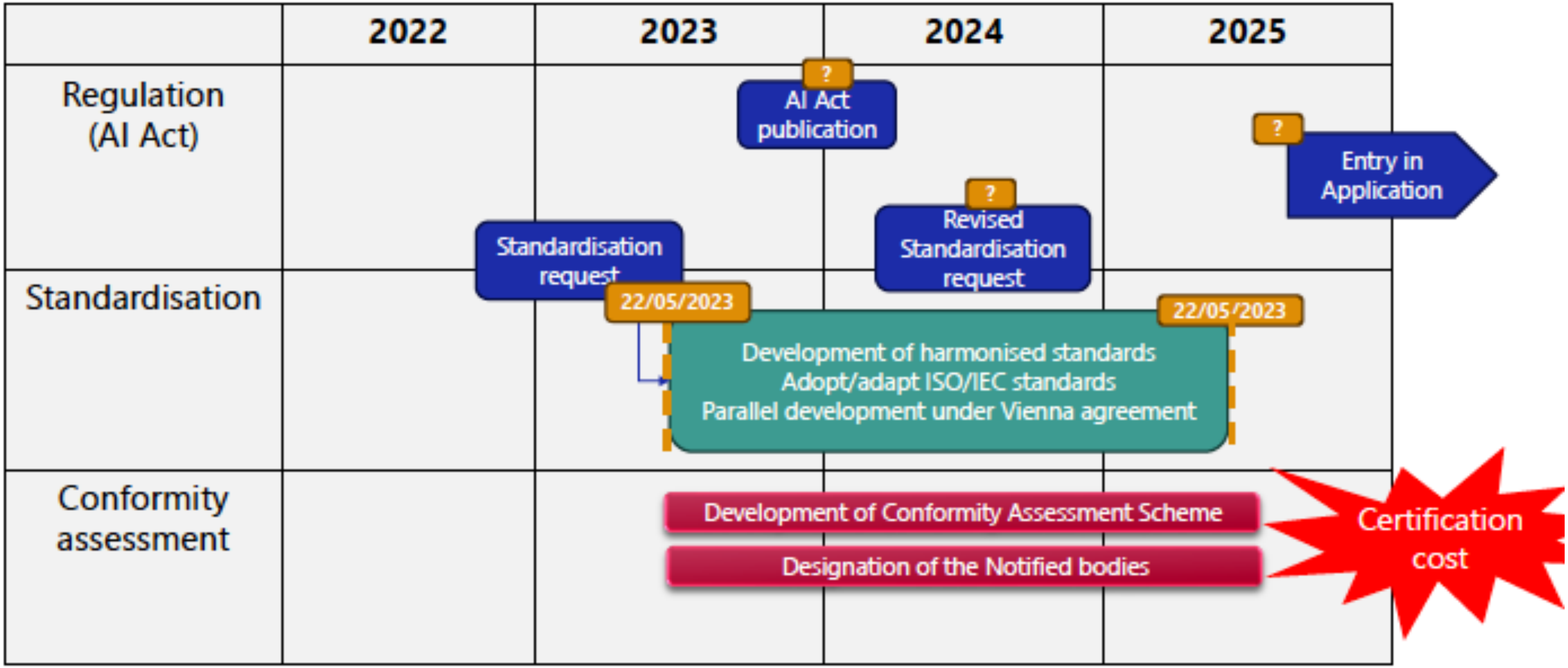
- Do we use the same scale ? - Measurement standards for AI

Measurement standards set points of reference upon which measurement equipment, testing, and performance standards can be built.

- Can systems talk to each other ? - Compatibility and interoperability

Interface and networking standards ensure that products and systems can work together, increasing the scope and usability of products and systems, and reducing waste and duplication

- CEN/CENELEC has two years to complete the standardisation request
  - If not complete it might get an extension, or EC will choose to develop “common standards”.
  - Two years is a very tight schedule considering the ESOs ways of working.



2022

2023

2024

2025

Regulation (AI Act)

Standardisation

Conformity assessment

?

AI Act publication

?

Entry in Application

?

Revised Standardisation request

Standardisation request

22/05/2023

22/05/2023

Development of harmonised standards
Adopt/adapt ISO/IEC standards
Parallel development under Vienna agreement

Development of Conformity Assessment Scheme

Designation of the Notified bodies

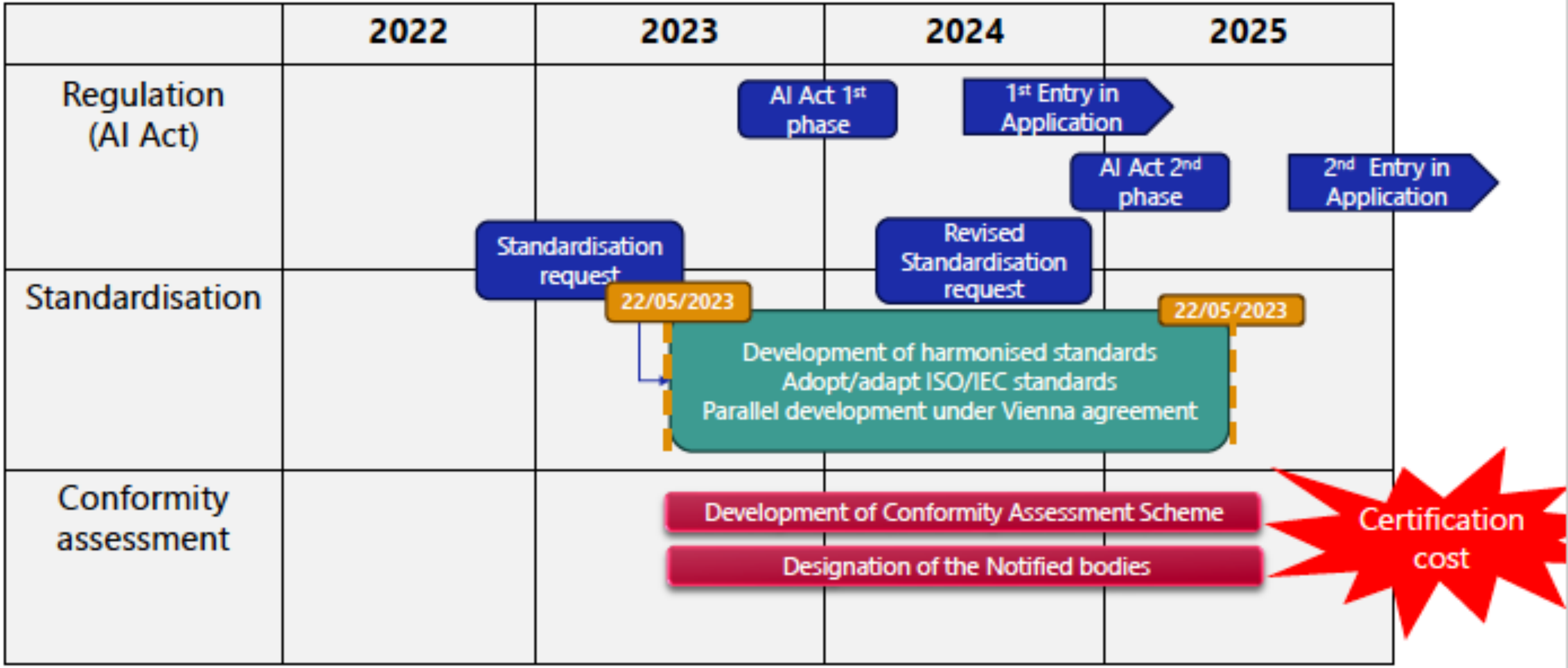
Certification cost

◆ Possible accelerated entry in application

- Several stages of AI Act.

Multilayer phase introduction, first phase could be : Forbidden use, transparency, logging

Standard and conformity assessment may not in place before application



2022

2023

2024

2025

Regulation (AI Act)

AI Act 1st phase

1st Entry in Application

AI Act 2nd phase

2nd Entry in Application

Standardisation

Standardisation request

22/05/2023

Revised Standardisation request

22/05/2023

Development of harmonised standards
Adopt/adapt ISO/IEC standards
Parallel development under Vienna agreement

Conformity assessment

Development of Conformity Assessment Scheme

Designation of the Notified bodies

Certification cost

10 Standardisation Requirements (SR) in the request

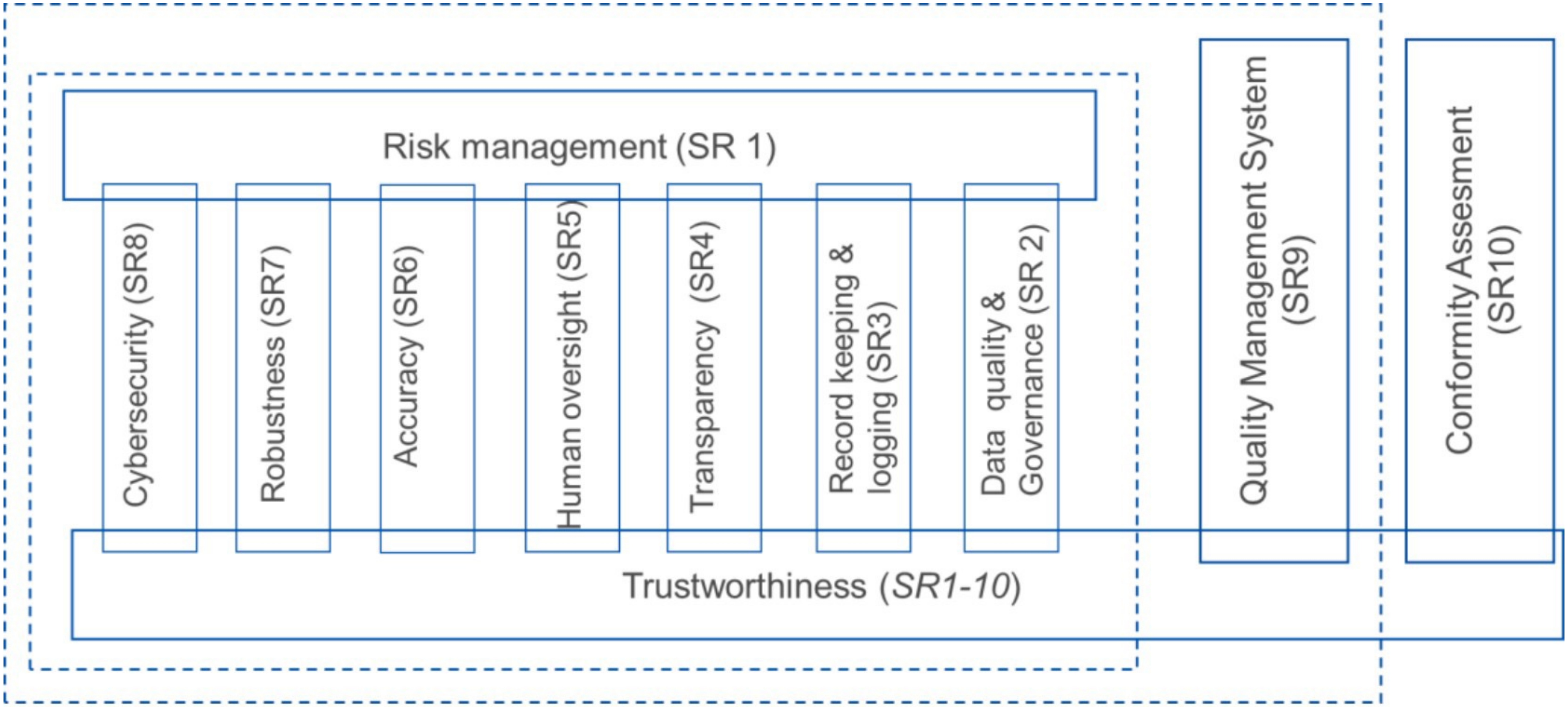
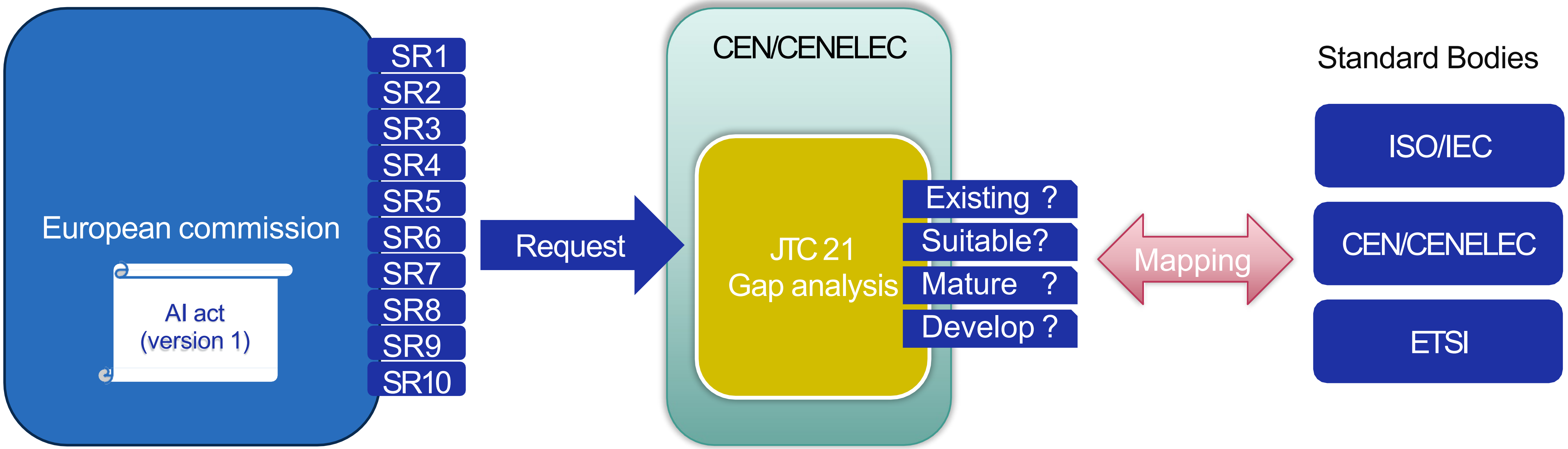


Figure 1: Architecture of Standards

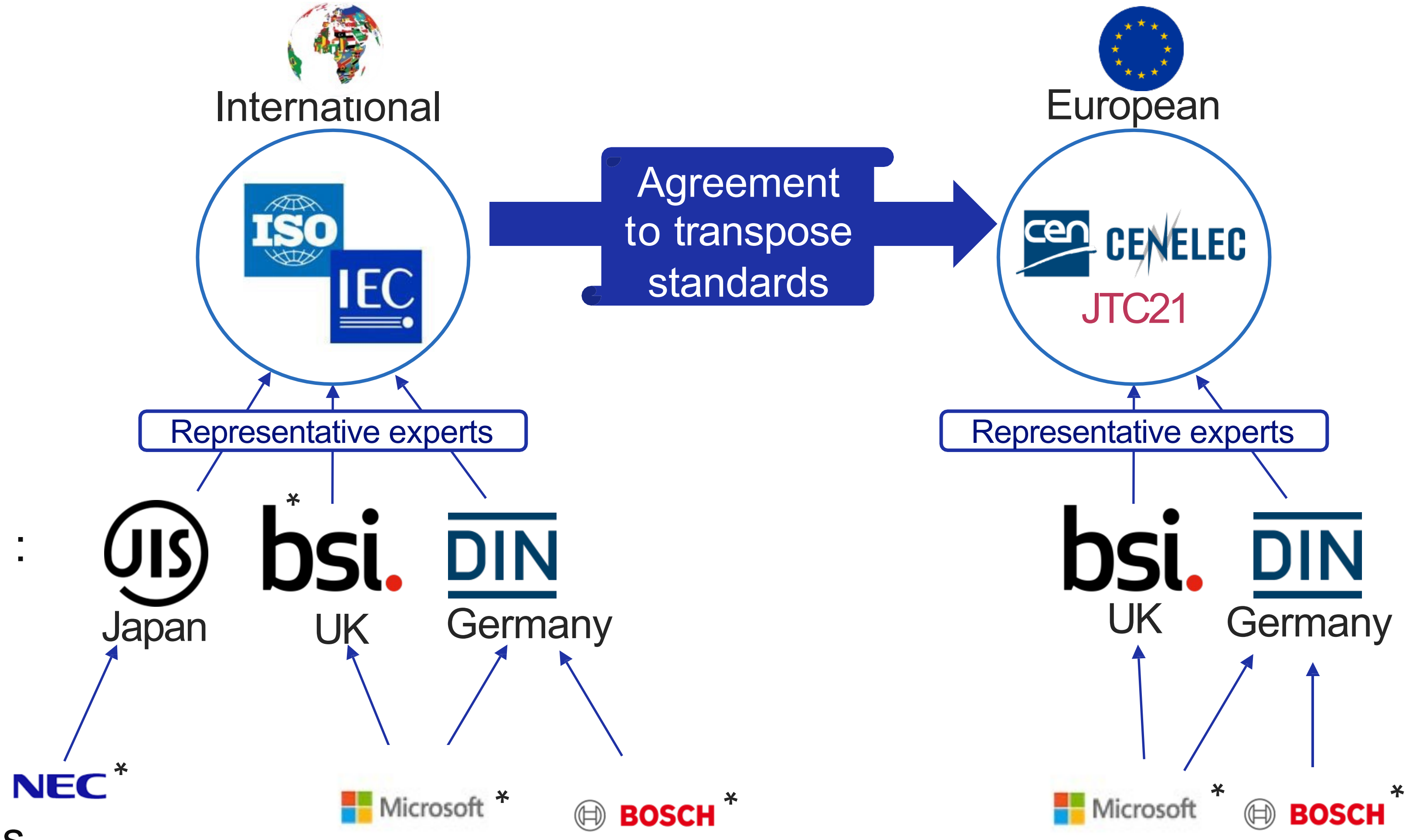
Standardisation gap analysis



- CEN/CENELEC has setup the committee JTC21 in charge to produce the standard for AI Act
- JTC21 is mapping existing standards with the SR requirements.
- JTC21 identifies gaps to be filled.

International standards and European standards

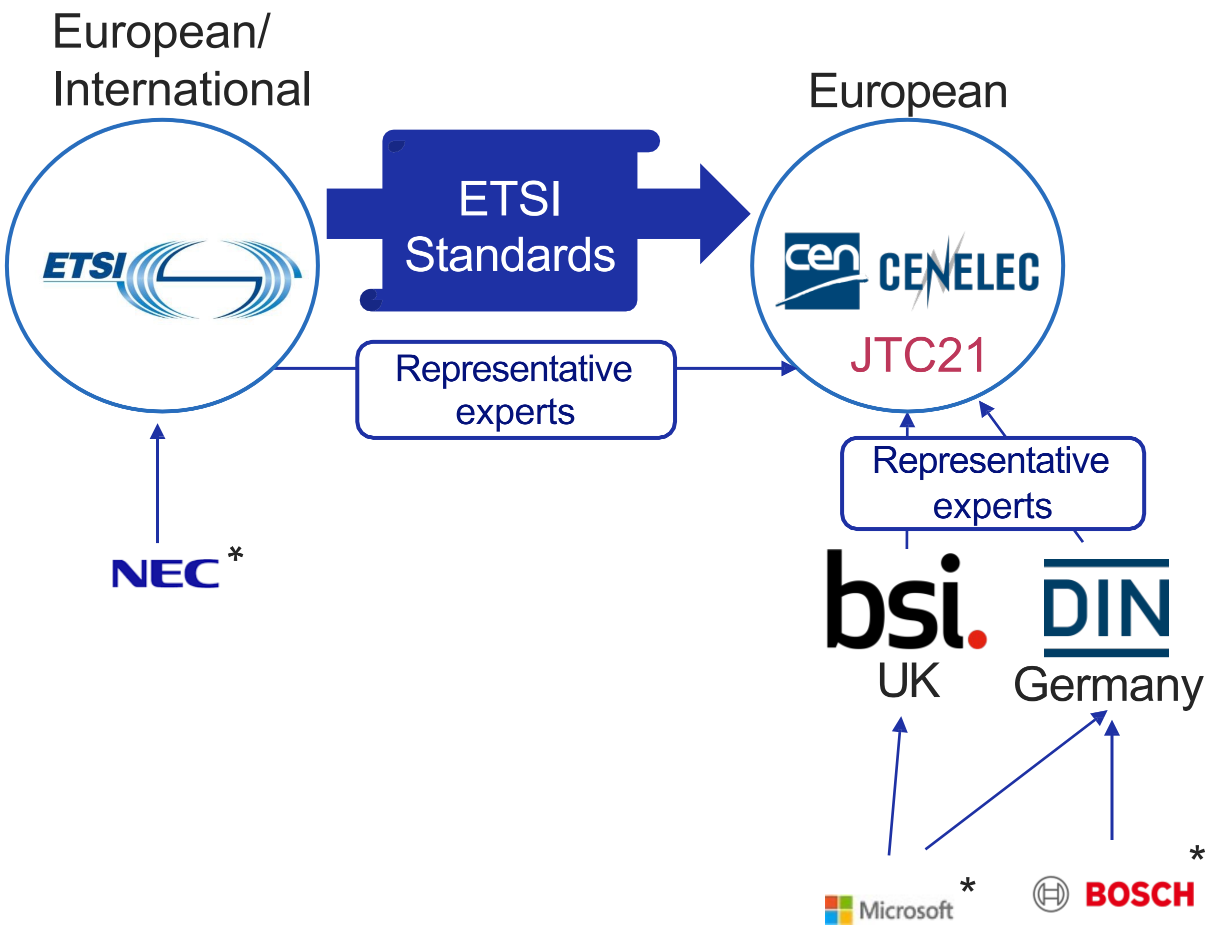
- CEN / CENELEC has a similar structure to ISO/IEC : national delegations with indirect representation
- Agreement to transpose international standard to European standards.
- Multinational companies send experts to influence work in several national delegations (eg : Microsoft)
- EC want to reuse international standard when possible
- National delegation model is rather slow to produce standards compared to industry member-based SDO



*Hypothetical example of participations

International standards and European standards

- The EC issued the standardisation to CEN / CENELEC request in May 2023, provided it collaborates with ETSI.
- ETSI experts participate in JTC21
- ETSI can produce harmonised European or international *standards
- Some ETSI standards are considered for AI Act, especially for cybersecurity



Gap examples : Cybersecurity

- EC added the security in the last draft of the AI Act.
- JTC21 has identified large gap in standards ecosystem
- Cybersecurity for AI standards in ISO/IEC are not mature.
  - ISO/IEC good at producing management standards (ex 27001 series)
  - ISO/IEC are not used to produce testing standards.
- Some ETSI are a possible candidate
  - ETSI Securing AI (SAI) group that has developed a set of TR which can be translated in harmonised standards, and produce testing standards (ETSI MTS)
  - ETSI has history of producing testing standards
- Testing is a major challenge.
  - Agile testing, continuous testing, “red teaming” is not part of the actual conformance testing
  - Skills to analyse the test

AI Act impact on business scenario

- AI Act still need to be finalised
  - AI Act may come in phases
  - We expect a second standardisation request to cover AI act Updates (LLM, GAI, FM …)
  - Management systems are quite mature and can be implemented now
  - Performance/measurements/testing is much more complex, and this will take time to be defined.

- JTC 21 standards gaps
  - JTC21 expectation for ISO/IEC standards to mature : This will take time due to process.
  - JTC21 expectation to start parallel development ISO/IEC : novel way, remain to be seen
  - Option that ETSI could fill some of the gap : May encounter resistance

- Possible delays :
  - JTC21 cannot produce the full standards in two years : Extension or alternative to be found

How to benefit from recognised standards specifications

Internal
Code of practice guidelines tools/specifications

+ Cost effective
+ Good PR / Prevent bad PR
+ "Good will" in case of litigations.
+ Early adopter of pre-standards.
+ Reduce internal errors
+ Better than nothing

Internal
Audits/conformance standards

+ Avoid or reduce cost of external third part
+ Pre-conformance reduce risk to fail.
+ Reduce internal errors
+ Early adopter of (pre-) standards.

External
Independent third party audits /conformance standards

- Expensive
- Only way for high-risk applications

Conclusion :
Reduce the risk and build trust with standards

Monitoring

- Monitoring progress of standard development
- Monitoring Conformity constraints
- Monitoring tools becoming available

Planning

- Risk management analysis of business cases
- Start with practical approaches and gradually expand towards certification
- Low risk use-case as PoC
- Influencing standards / pre-standardisation (tools …)

Implementing

"Trust goes beyond compliance"

- Implement specifications/guidelines when practical
- Implement management system (risk, process…)
- Implementing early features for compliance (logging / documenting / test / statistic)
- Prepare the expertise for auditing and cyber testing

Main standardisation bodies considered for AI Act

One International body

Organization for Standardisation (ISO)
International Electrotechnical Commission (IEC)

International body,
Indirect representation with national delegations

Three European bodies

European Committee for Standardisation
European Committee for Electrotechnical Standardisation

European body,
Indirect representation with national delegations

European Telecommunications Standards Institute

European and international
Direct member representation

DISCUSSION

Standards play a key role in the uptake of new technologies: among challenges

(A) time to develop standards

(B) lack of industry expert capacity

(C) access (payment model) and

(D) obsolescence.

Types of standards:

(1) foundational and terminology standards

(2) management/process standards

(3) performance standards

(4) measurement standards

(5) compatibility/interoperability standards.

DISCUSSION

Previous regulations were focused on measurable requirements that could be more easily reflected into standards.

- Today it’s more difficult to translate functional requirements (e.g. AI ethics) into standards. How to standardise values?

Crypto algorithms are an interesting new area of standardisation.

International cooperation needed to create interoperable conformity assessment schemes.

Market access: lack of standards, creation of EU specific requirements and/or common specifications that become a barrier to enter the EU market.

DISCUSSION

Lack of metrics and or diverse metrics for measuring trustworthiness elements (e.g. security, safety and privacy).

- Need for integrated approaches.

Multidisciplinary approaches are needed to capture current multifaceted challenges of technologies

Trust: brand is an element of trust.

- Not all qualifiers can be addressed by regulations.
- Banking sector, mobile phones are a good example.

Inclusion of academia is critical.

DISCUSSION

More research is required before standards achieve explainability

Can European values be incorporated into standards – or should it be left up to industry? And how do they figure with US companies which heavily influence ISO?

Open source is the other side of the argument. Google and others are trying to capture the higher ground by pushing tools rather than standards which jeopardises instead

DISCUSSION

Trust categories based on:

- Geographical
- Brand / marketing
- Compliance
- Risk
- Audience

Global levels of trust equate to the lowest level of trust

And supply chains are global …

There are different trust levels on data – which are vital for maintaining data sovereignty

DISCUSSION

Skills are essential to perform conformity assessments by notified bodies, to create certification schemes, and to train those who will assess compliance.

- There is a lot of recruitment in the area of AI in anticipation

Common criteria have some limited application.

- The only way for common criteria and other standards to be global is to build consensus at the lowest level of trust.

PRIORITIES

Resources for creations of international standards and for implementation of regulations

Talent and skills

Interoperability, composability (standard-agnostic)

Interoperability of regulations

Create trust across supply chain and specific sectors

Greater communication on standards

Understanding what trust means for customers

Expert knowledge to develop standards e.g. explainability

Scientific and user centric approach to technologies

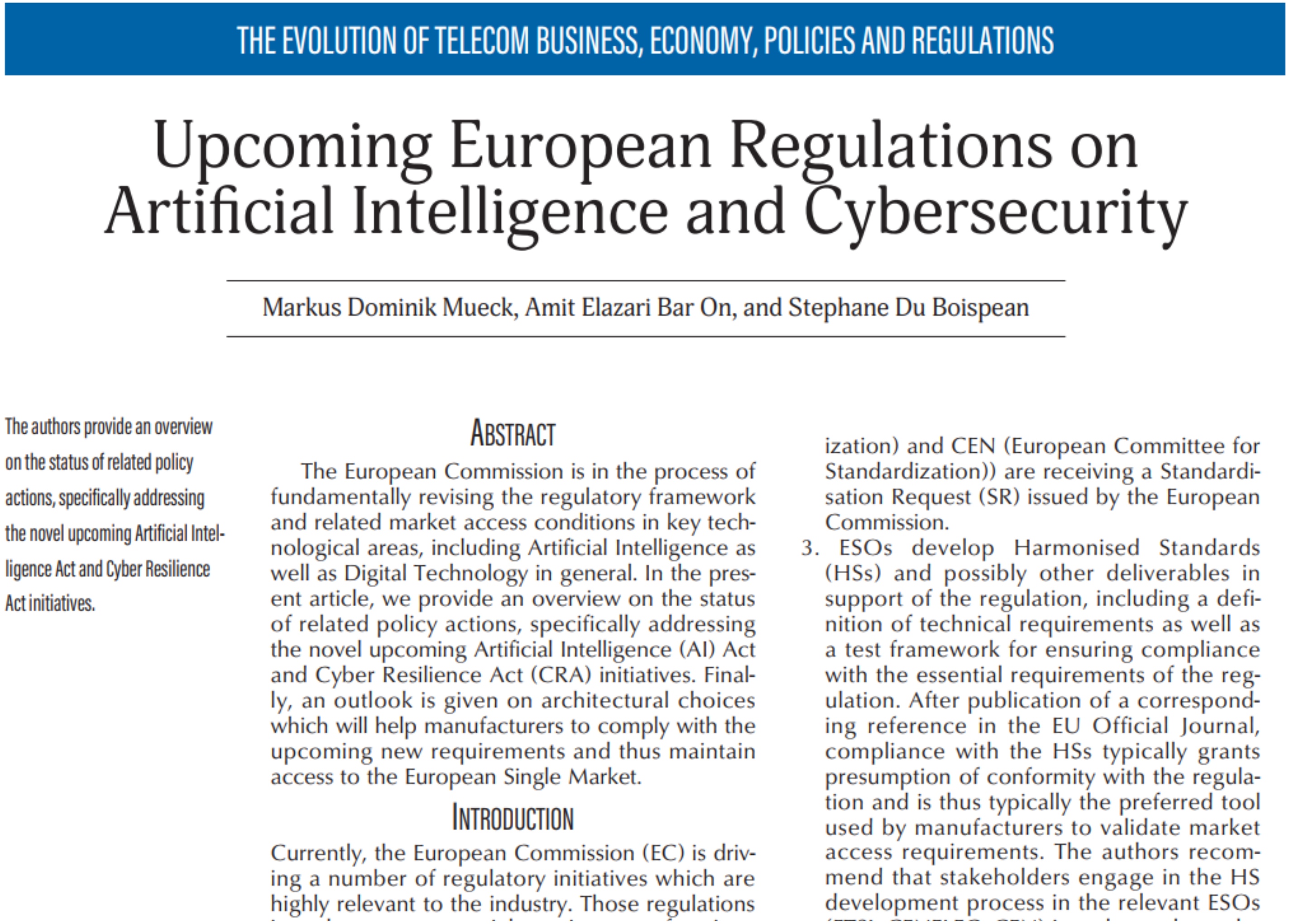
Metrics

Open-source environment

REFERENCE ARTICLE

SCAN ME

https://ieeexplore.ieee.org/document/10061649



THE EVOLUTION OF TELECOM BUSINESS, ECONOMY, POLICIES AND REGULATIONS

Upcoming European Regulations on Artificial Intelligence and Cybersecurity

Markus Dominik Mueck, Amit Elazari Bar On, and Stephane Du Boispean

The authors provide an overview on the status of related policy actions, specifically addressing the novel upcoming Artificial Intelligence Act and Cyber Resilience Act initiatives.

Abstract

The European Commission is in the process of fundamentally revising the regulatory framework and related market access conditions in key technological areas, including Artificial Intelligence as well as Digital Technology in general. In the present article, we provide an overview on the status of related policy actions, specifically addressing the novel upcoming Artificial Intelligence (AI) Act and Cyber Resilience Act (CRA) initiatives. Finally, an outlook is given on architectural choices which will help manufacturers to comply with the upcoming new requirements and thus maintain access to the European Single Market.

Introduction

Currently, the European Commission (EC) is driving a number of regulatory initiatives which are highly relevant to the industry. Those regulations

ization) and CEN (European Committee for Standardization)) are receiving a Standardisation Request (SR) issued by the European Commission.

3. ESOs develop Harmonised Standards (HSs) and possibly other deliverables in support of the regulation, including a definition of technical requirements as well as a test framework for ensuring compliance with the essential requirements of the regulation. After publication of a corresponding reference in the EU Official Journal, compliance with the HSs typically grants presumption of conformity with the regulation and is thus typically the preferred tool used by manufacturers to validate market access requirements. The authors recommend that stakeholders engage in the HS development process in the relevant ESOs

TRUST
IN
DIGITAL
LIFE

THANK YOU!

trustindigitallife.eu