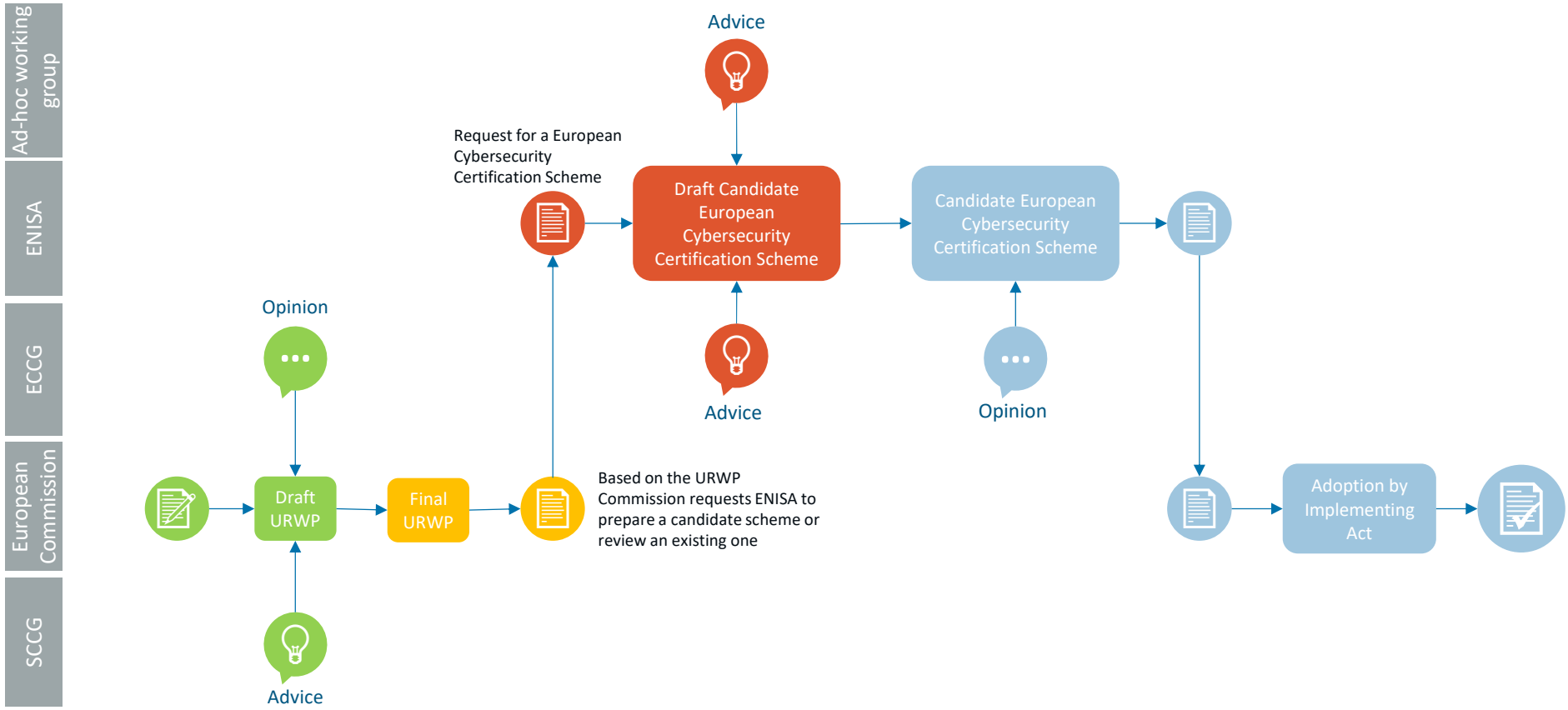
Security Conference

# Cybersecurity landscape: a narrow scope view

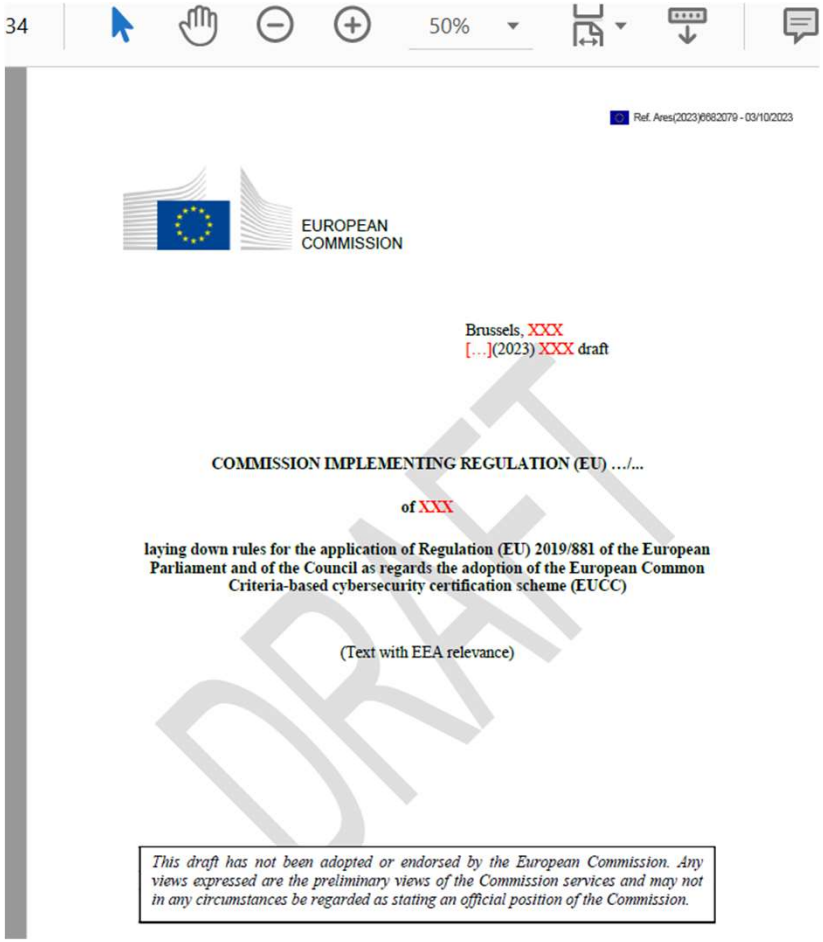
Dr Andreas MITRAKAS, Head of Unit “Market, Certification & Standardisation”, ENISA

16/09/2023

# Go with the (cybersecurity certification) flow



# EUCC: In public feedback (Come in droves)



34 50%

Ref. Ares(2023)6682079 - 03/10/2023

EUROPEAN COMMISSION

Brussels, XXX
[…](2023) XXX draft

**COMMISSION IMPLEMENTING REGULATION (EU) …/...**

**of XXX**

**laying down rules for the application of Regulation (EU) 2019/881 of the European Parliament and of the Council as regards the adoption of the European Common Criteria-based cybersecurity certification scheme (EUCC)**

(Text with EEA relevance)

DRAFT

*This draft has not been adopted or endorsed by the European Commission. Any views expressed are the preliminary views of the Commission services and may not in any circumstances be regarded as stating an official position of the Commission.*

1 / 18 66.7%

Ref. Ares(2023)6682079 - 03/10/2023

EUROPEAN COMMISSION

Brussels, XXX
[…](2023) XXX draft

ANNEXES 1 to 7

**ANNEXES**

**to the**

**COMMISSION IMPLEMENTING REGULATION**

**laying down rules for the application of Regulation (EU) 2019/881 of the European Parliament and of the Council as regards the adoption of the European Common Criteria-based cybersecurity certification scheme (EUCC)**

# EUCS: a scheme for all ~~seasons~~ stakeholders

## All capabilities

Also based on ISO/IEC 22123

All cloud capabilities are supported: Infrastructure, Platform, Application

Covers the full stack

No mention of deployment model

## Horizontal

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)

## 3 assurance levels

As defined in the European Cybersecurity Act

‘basic’

‘substantial’

‘high’

All levels based on an assessment by an accredited third-party

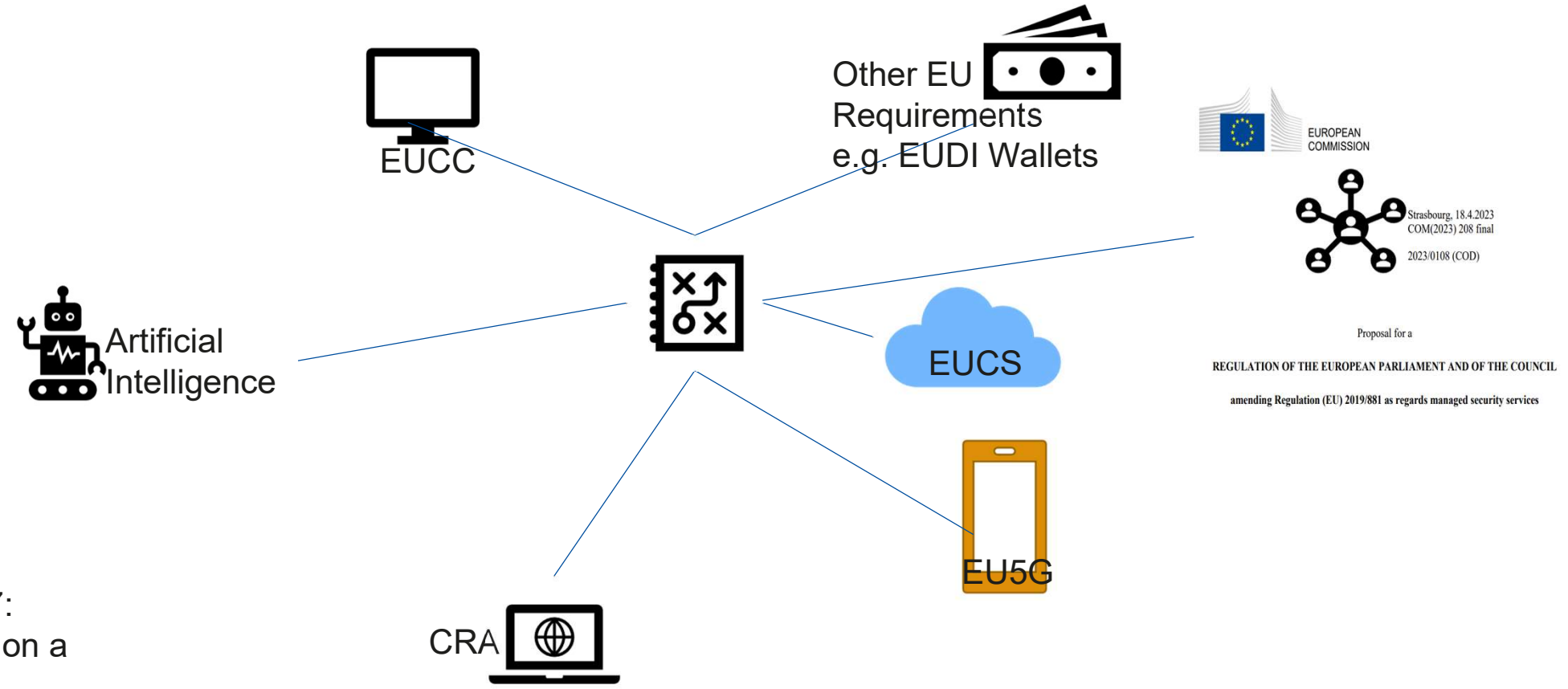
# EU5G: Are we there yet?

- **ENISA expects the first draft of the scheme to be available for public review in late Q4 2023**
- **The AHWG supporting ENISA has been retained from the initial phase; it comprises of a broad selection of relevant stakeholders (around 100 participants):**
  - **eUICC and network products developers**
  - **CABs**
  - **MNOs**
  - **standardisation organisations ETSI, CEN CENELEC**
  - **public authorities (MNO, NCCA, regulators)**
  - **Continuous collaboration with GSMa and 3GPP with the indispensable support of ETSI**

# EU5G: Q4 sprint

- **Valid input from GSMa NESAS, SAS-SM, SAS-UP and eUICC, plus mitigation based on risk assessment, gap analysis previously carried out**
- **Close coordination with the ECCG and the EU NIS Cooperation Group allows to reuse their elements for the benefit of the EU5G scheme**
- **Multiple challenges:**
  - **estimate the equivalent CSA assurance level of existing GSMA schemes and ensure consistency across assurance levels concerning 5G components to be certified**
  - **Carry out risk assessments with comparable assumptions on intended use of 5G components, to potentially ensure technical comparability between GSMA/3GPP and EU schemes**
  - **future maintenance of the scheme (respective role of ENISA/3GPP/GSMA)**
  - **Navigate and coordinate across heterogeneous stakeholders**
  - **Manage expectations of a global group of stakeholders**

# Certification: how does it all fit together?

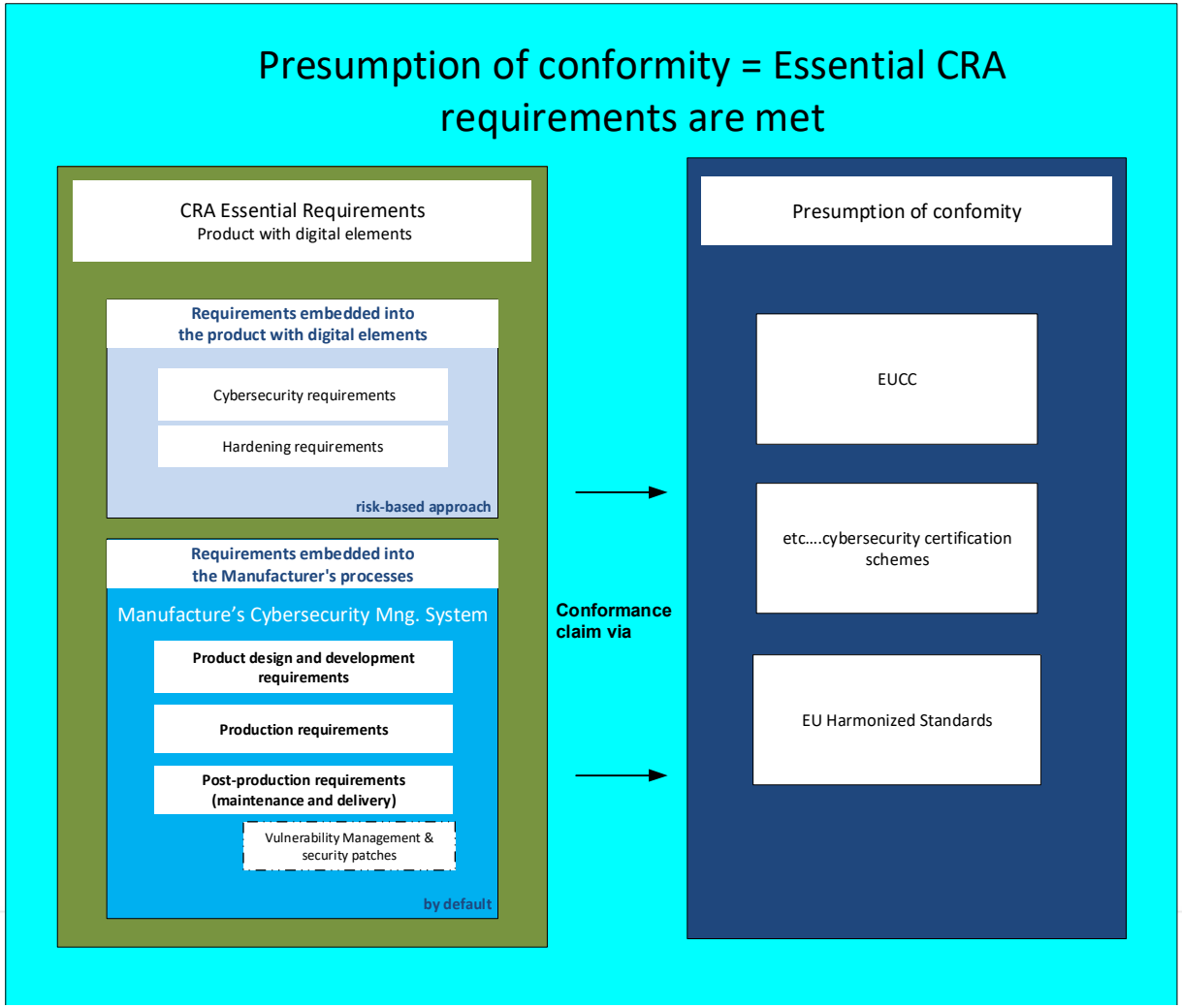



prEN18037: Guidelines on a sectoral cybersecurity assessment

# CRA: building further on presumption of conformity

Pursuant to a risk assessment, manufacturers can choose whether to demonstrate conformity based on:

- harmonised standards i.e. Decision 768/2008
- EU cybersecurity certification schemes or parts thereof
- A combination thereof
- Or by other means if they do not apply harmonized standards



# AI: Use cases

## Medical imaging →AI Act +sectorial

A private clinic buys access to a **cloud-based AI platform** that allows training a ML model on patients' medical imagines (X-rays) and on data related to age, gender and body mass. The private clinic develops a **ML-based tool** to detect the presence or absence of osteoporosis in patients. The private clinic sells the tool to other private clinics.

## Behavioral biometrics at the work place →CRA+AI Act

A private company has deployed an **AI-based identification system** to monitor the presence of its employees. To do so, the company, based on biometric data obtained from the employees' keystrokes, determines if the identified employee is present.

The AI-system has been bought from an external company.

## Personal assistant device →CRA

A private company is putting on the market a personal assistance device that embeds an AI-based solution that can understand a user's requests when the user speaks to it, and delivers the service requested by the user. The speech processing algorithm has been developed in-house.

Two sub use cases:

a) The device is **autonomous/stand-alone** (local data handling and processing)

b) The device relies on a **cloud-based solution** for data handling and processing

## Water quality monitoring →CRA + AI + NIS2

A private company which is the supplier and distributor of water for human consumption deploys an **AI system to monitor water cycle data**, including checking the water quality. In case the quality of the water is insufficient, the AI system automatically regulates (block or ration) the supply of water and calculates data supply cycles.

The system has been developed by a private company specifically for the supplier/distributor.

# Study on supply chain standards

- Overview of threats and risks to the supply chain of ICT equipment and services by (primarily) malicious actors
- Review of the differences between the software and hardware supply chains of any single piece of ICT equipment
- Recommendations on means to protect the supply chain from the actions of malicious actors
- Advice to build trusted supply chains – with focus on standards

# What does this all mean for standardization?

**Standards needed for compliance**

**Gaps in current standards compared to upcoming requirements**

**International alignment in standards to facilitate market access**

**Market analysis needed to determine new requirements for standards**

**Multitude of roles for cybersecurity**

**Growing role of private entities in standardization**

**PDCA**

# THANK YOU