jtsec

Applus

jtsec

Applus+

Using EUCC to meet CRA

ICCC 2024

DOHA, QATAR

About me

- **José Manuel Pulido:**
- Common Criteria expert and Consulting Manager in jtsec.
- CCToolbox developer
- Contributor to ENISA, Eurosmart and ISO projects and CEN/CENELEC.
- More than 12 years of experience in cybersecurity technologies
- Speaker at several conferences including CCUF20, ICCC20, ICCC21, ICC22, ICC23.

About us

jtsec Applus

- jtsec is part of the A+ group along with Lightship Security. We have labs in Canada, USA and Spain.
- Cybersecurity **evaluation** & consultancy **services**
- Common Criteria, LINCE and ETSI EN 303 645 accredited lab.
- Developers of the most powerful tool for Common Criteria, CCToolbox.
- **Involved in standardization** activities (ISO, CEN/CENELEC, ISCI WGs, ENISA CSA WGs, CCUF, CMUF, ERNCIP, …)
- Members of the SCCG (Stakeholder Cybersecurity Certification Group)

Background

- In July 2023, the **European Commission requested ENISA's** technical support for implementing the Cyber Resilience Act (CRA).
- ENISA prepared a report proposing a strategy **to meet with CRA through EUCC certification**.
- The first version, released in November 2023, presented in ENISA Cybersecurity certification week (Malaga, November 2023).
- The report was updated in **2024**, in response to legislative developments, including **changes in the CRA (March 2024)** and the publication of the **EUCC Implementing Act**. Later **distributed to ECCG and SCCG** and updated in October.
- The report serves as an initial analysis, aiming to inform future decisions on how EUCC certification could demonstrate compliance with the CRA.

EU Cyber Resilience Act (CRA) - Overview

What is CRA? - (EU) 2019/1020

- A regulatory framework enforcing cybersecurity requirements for products with digital elements across the EU.

Scope of application

- Products with digital elements (hardware and software) and their remote data processing solutions.
- … virtually any digital device, ranging from smart toys to security ICs.

Key obligations for Manufacturers

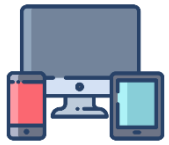
- Conduct cybersecurity risk assessments
- Provide security updates for up to 10 years.
- Report vulnerabilities within 24-72 hours to ENISA.

Deadlines

- 10/10/2024 – Adopted by the Council
- Next publication at the Official Journal of the EU in 1-3 months
- 20 days after: entry into force
- 36 months after: regulation will apply (January 2028).

EU Cyber Resilience Act (CRA) - Overview

Essential Security Requirements (Annex I)



Part I: product security functions

Secure by default conf.
Timely automatic updates.
Access control/auth.
Data minimization.
Resilience – DoS
Reduced attack surface
Secure data removal

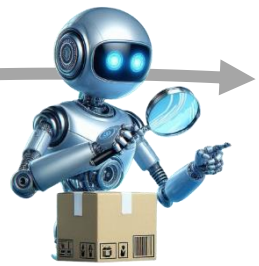
Part II: manufacturer's Vulnerability handling

SBOM
Remediation & disclosure
Security vs functional updates
Security review & testing
Timely and free…

Selectable / applicable based on risk assessment

Always mandatory

CRA Conformity Assessment



CRA Product categories

Criticality

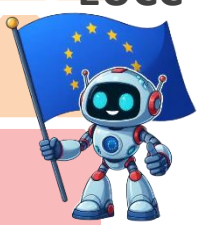
90% of products	10% of products		
Products with digital elements	**Important "Class I"**	**Important "Class II"**	**Critical**
Criteria: n/a	**Annex III** Password managers, SIEM, Network Management, Operating systems, routers etc.	**Annex III** Hypervisors Firewalls, IDS; Tamper-resistant microprocessors; Tamper-resistant microcontrollers.	**Annex IV** Hardware Devices with Security Boxes Smart meters Smartcards
Internal control procedure - **Module A** (Self-assessment)			

EU-type examination procedure **(Module B)** + EU-type internal production control (**module C**)

Full quality assurance (**module H**)

CSA European Cybersecurity Certification Scheme (**substantial**)

EUCC



Strictness

CRA Essential Security Requirements vs EUCC

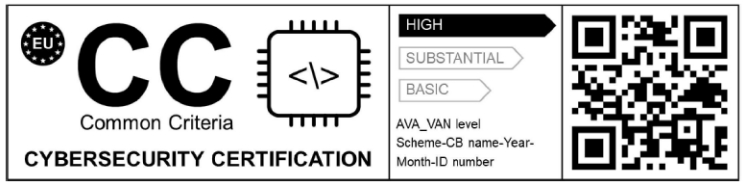
CRA

Compliance ->

- Essential Cybersecurity Requirements (Annex I)

Equivalence between ESRs and CC technical elements?

Then the EUCC certification **demonstrates compliance** with CRA ESRs



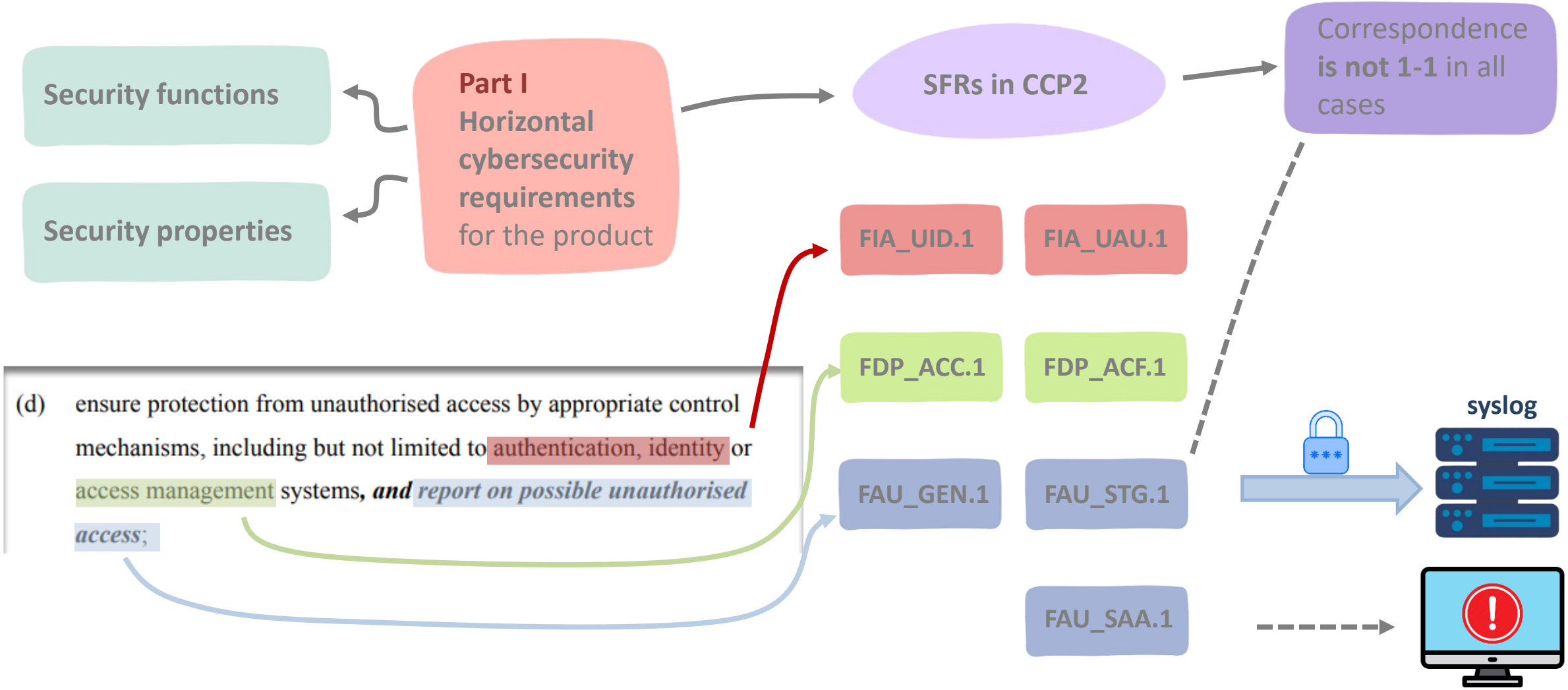
Compliance ->

- Technical elements:
  - ✓ **SFRs** are met by EUCC TOE
  - ✓ **SARs** driving the EUCC evaluation
- EUCC obligations for manufacturer
- Assessed by 3rd party CAB

CRA Article 27 (8)

*Products with digital elements and processes put in place by the manufacturer for which an EU statement of conformity or **certificate has been issued under a European cybersecurity certification scheme** adopted pursuant to Regulation (EU) 2019/881, shall be **presumed to be in conformity with the essential requirements set out in Annex I** in so far as the EU statement of conformity or **European cybersecurity certificate, or parts thereof, cover those requirements.***

CRA ESRs: Annex I Part 1 & EUCC technical elements



CRA ESRs: Annex I Part 1 & EUCC technical elements

Security functions

Security properties

Part I
Horizontal cybersecurity requirements
for the product

SFRs in CCP2

Correspondence **is not 1-1** in all cases

Horizontal requirements can be met in various ways in across different vertical scenarios

A.PHYS-PROTECTION

Stored user passwords or private keys

FDP_SDC.1

FCS_COP.1

T.PHYS-MANIPULATION

Private keys
Biometrics
PIN
Certificates

FPT_ITT.1

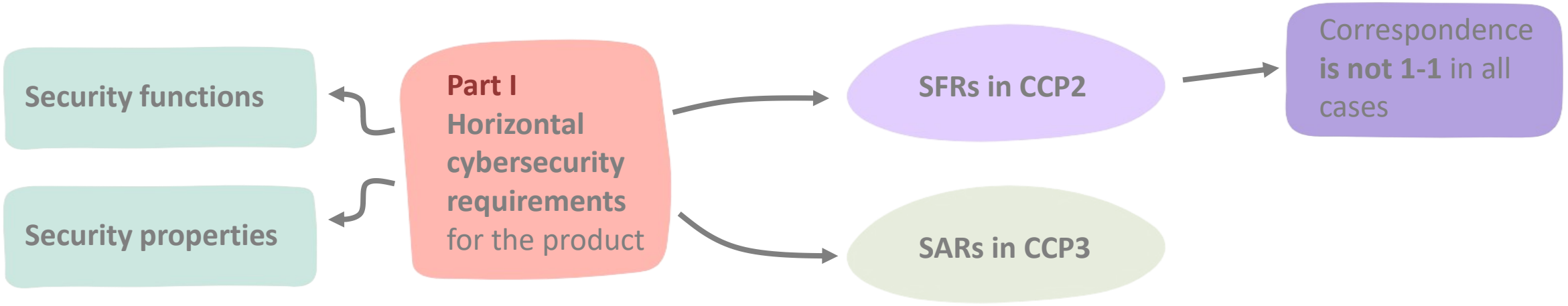
FPT_PHP.3

FDP_ITT.1

FDP_ACC.1

(e) protect the confidentiality of stored, transmitted or otherwise processed data, personal or other, such as by encrypting relevant data at rest or in transit by state of the art mechanisms, ***and by using other technical means***;

CRA ESRs: Annex I Part 1 & EUCC technical elements



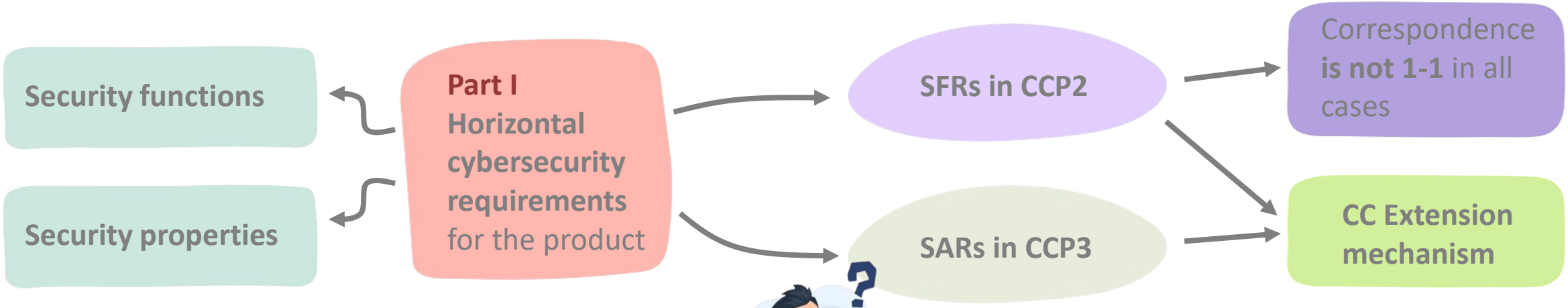
(j) be designed, developed and produced to limit attack surfaces, including external interfaces;

AVA_VAN.1

ADV_FSP.1

AGD_OPE.1

CRA ESRs: Annex I Part 1 & EUCC technical elements



(g) process only data, personal or other, that are adequate, relevant and limited to what is necessary in relation to the intended ***purpose*** of the product ***with digital elements*** (data minimisation);

ADV_PDM: Processed data minimisation	1

ADV_PDM.1.1C **The rationale for data minimisation shall identify all user data that is processed by the TOE.**

ADV_PDM.1.2C **The rationale for data minimisation shall relate each user data processed by the TOE with the input interfaces from which it is received and with the outbound interfaces where it is outputted to non-TOE entities.**

ADV_PDM.1.C **The rationale for data minimisation shall demonstrate that all user data processed by the TOE is necessary and adequate in relation with the intended purpose of the TOE.**

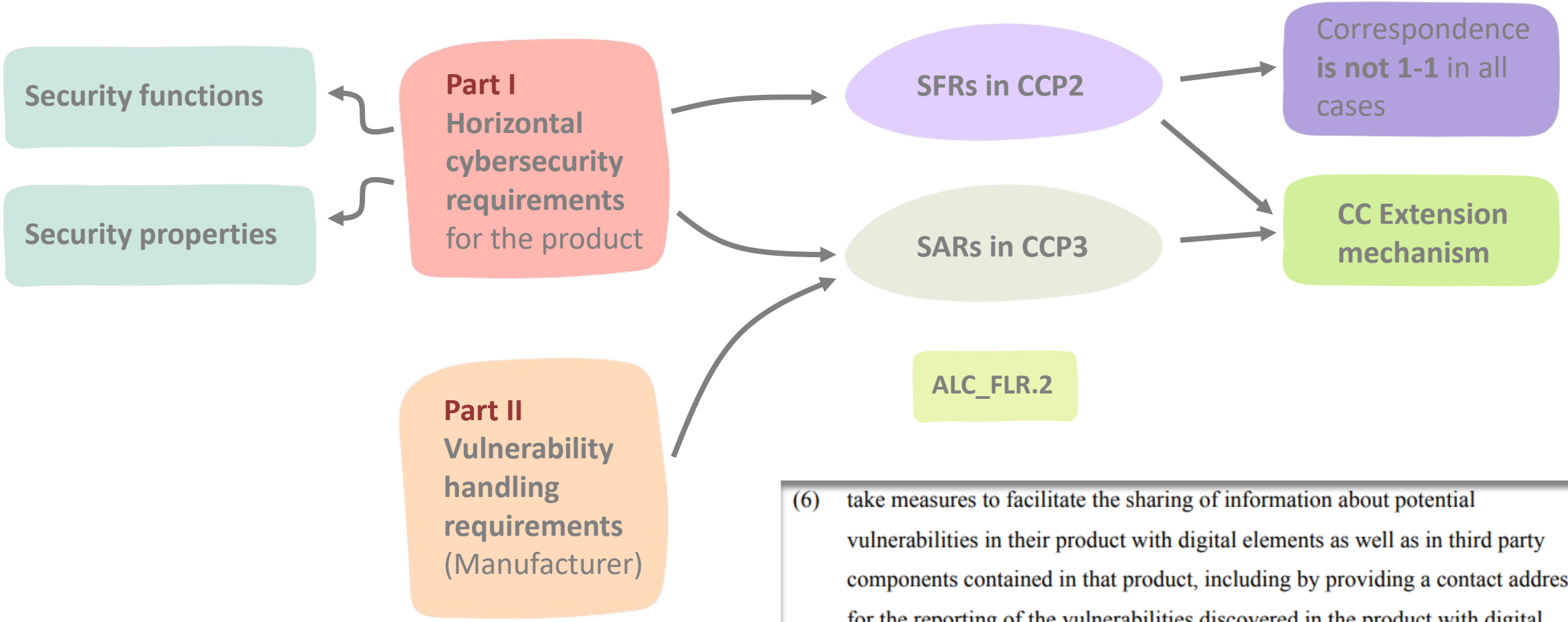
Work Unit ADV_PDM.1-2

The evaluator ***shall examine*** the rationale for data minimisation and the operational user guidance, in order to determine that it provides relationships between all the user data processed by the TOE and the input interfaces from which the data is received and with the outbound interfaces through which it is outputted to non-TOE entities.

Work Unit ADV_PDM.1-3

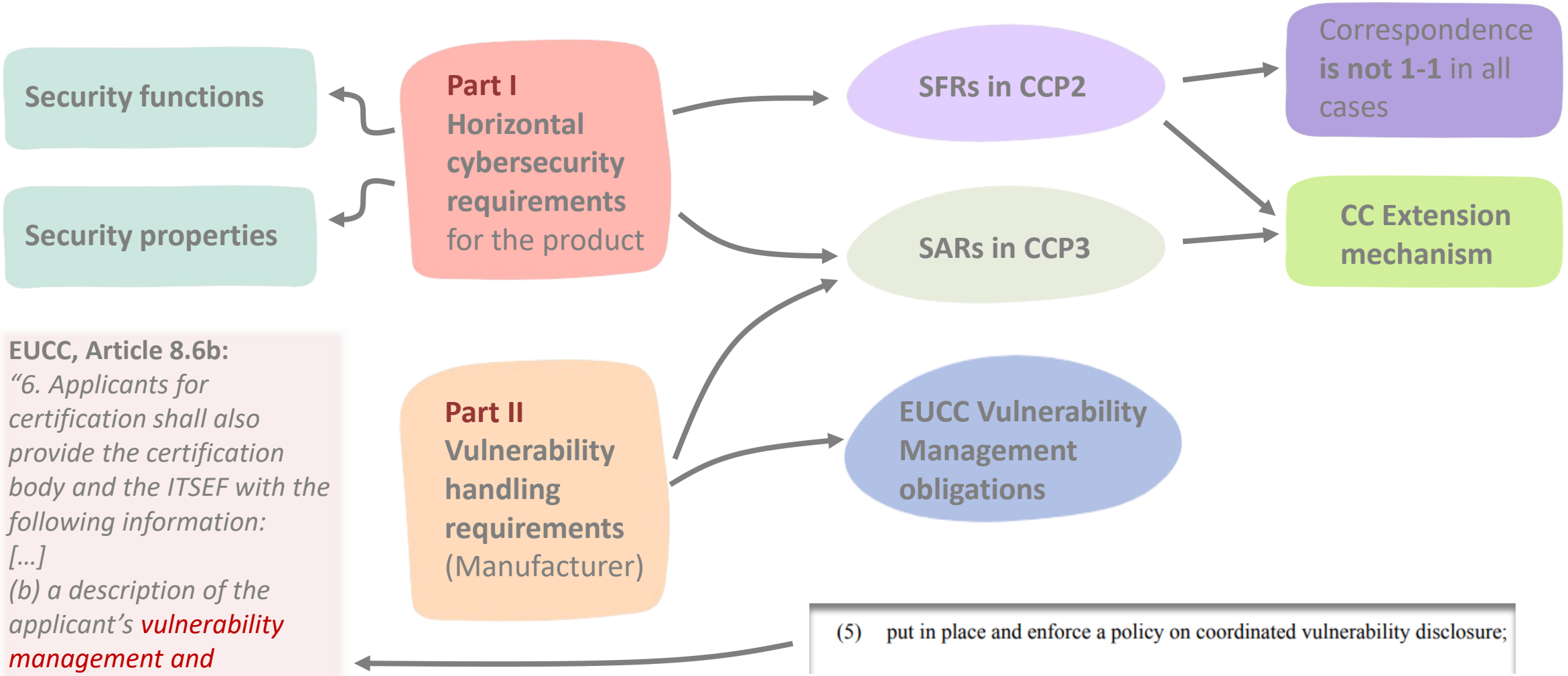
The evaluator ***shall examine*** that the rationale for data minimisation and the operational user guidance in order to determine that the user-accessible interfaces in the user operational guidance don't indicate the existence of other user data processed by the TOE that is not declared in the rationale for data minimisation.

CRA ESRs: Annex I Part 2 & EUCC technical elements



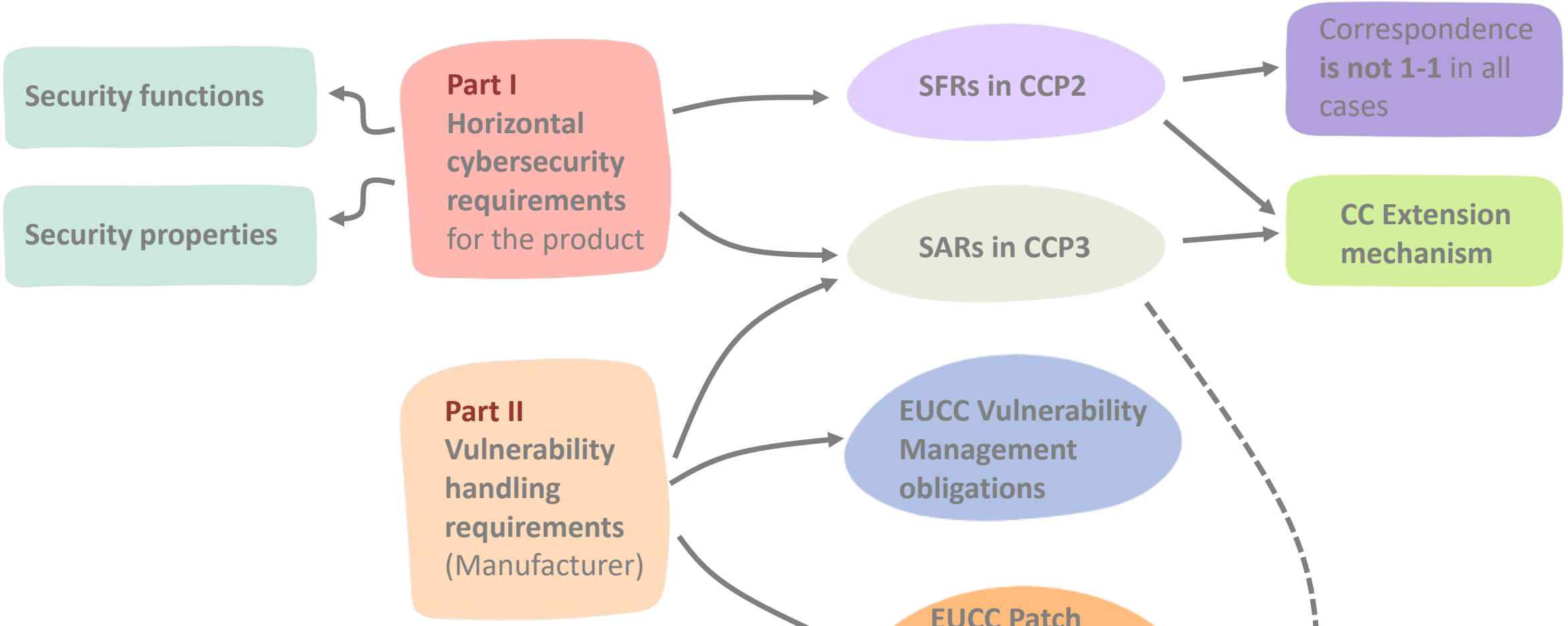
(6) take measures to facilitate the sharing of information about potential vulnerabilities in their product with digital elements as well as in third party components contained in that product, including by providing a contact address for the reporting of the vulnerabilities discovered in the product with digital elements;

CRA ESRs: Annex I Part 2 & EUCC technical elements



EUCC, Article 8.6b:
"6. Applicants for certification shall also provide the certification body and the ITSEF with the following information:
[…]
(b) a description of the applicant's vulnerability management and vulnerability disclosure procedures.

CRA ESRs: Annex I Part 2 & EUCC technical elements



(7) provide for mechanisms to securely distribute updates for products with digital elements to ensure that vulnerabilities are fixed or mitigated in a timely *manner* ***and, where applicable for security updates, in an automatic*** manner;

CRA Manufacturer's risk assessment

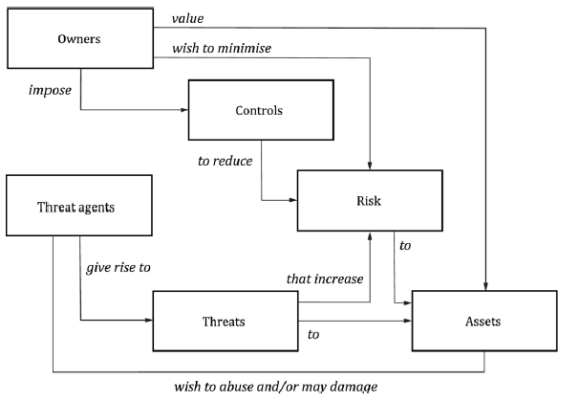
CRA Article 13: Manufacturer's cybersecurity risk assessment

Based on:
- *intended purpose*
- *reasonably foreseeable use*

It determines the **Applicability of ESRs** (**Annex I, Part I**)

How Annex I, Part II **vulnerability handling requirements are applied.**

CRA **does not mandate a specific risk assessment methodology** (further clarifications could be required in the future)



Risk assessment required as input to the CC Security Problem Definition

Selection of the AVA_VAN **attack potential** (CEM 2022 p. 464).

Security Problem Definition (assets, threats, environment..)

Security Problem Definition directly drives selection of SFRs equivalent to CRA ESRs is based on the SPD

Selection of SARs is indirectly linked with SPD (internal consistency statement in ASE_REQ.1.11C)

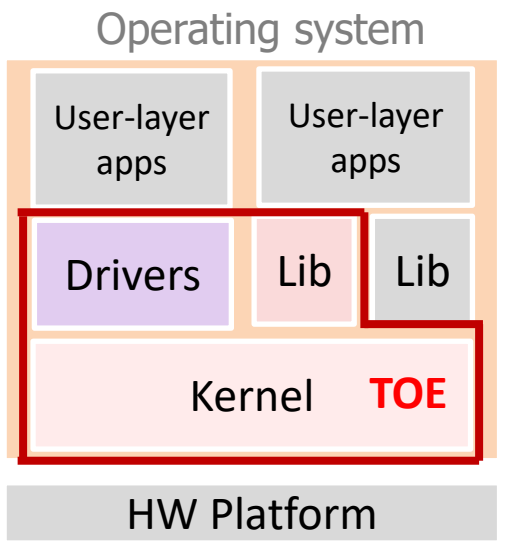
CRA scope vs EUCC TOE scope

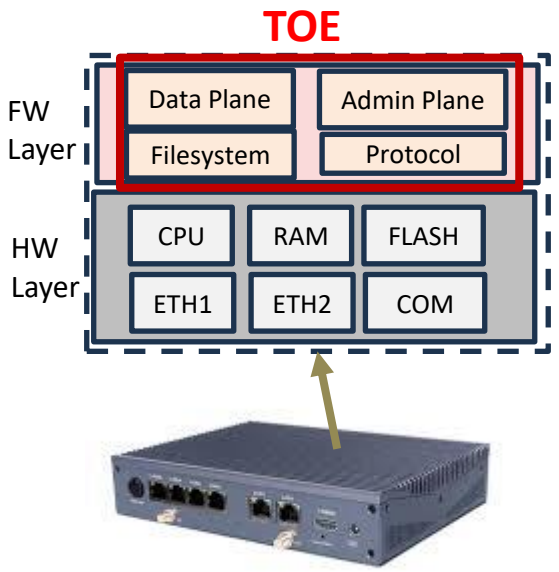
CRA Essential Cybersecurity Requirements and other obligations apply to the **scope** of the full **product with digital elements,** including **remote data processing solutions**

- **CC TOE scope is often smaller than the full product** placed on the market by the TOE manufacturer:
  - Limit assessment to the boundary of the security functions
  - Reduce attack surface
  - Time and cost proportional to scope size

- **Gap:** when the TOE scope is smaller, EUCC/CC certificate doesn't demonstrate CRA compliance for the full product placed on the market.

- **Main cases:**
  - **TOE Distributed Separately** (from non-TOE components):
    - ✓ Compliance of non-TOE with CRA demonstrated **through other methods** (e.g., European harmonized standards).
  - **TOE & Non-TOE Distributed Together / coupled architecture**:
    - ✓ Enlarging TOE may not always be feasible.
    - ✓ Key Question: Does the TOE scope protect the full product?

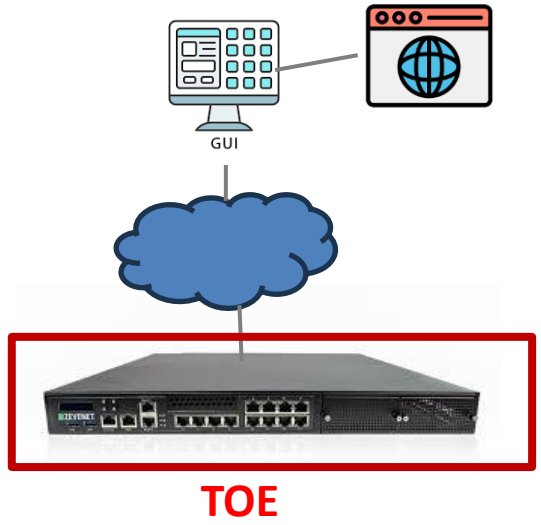




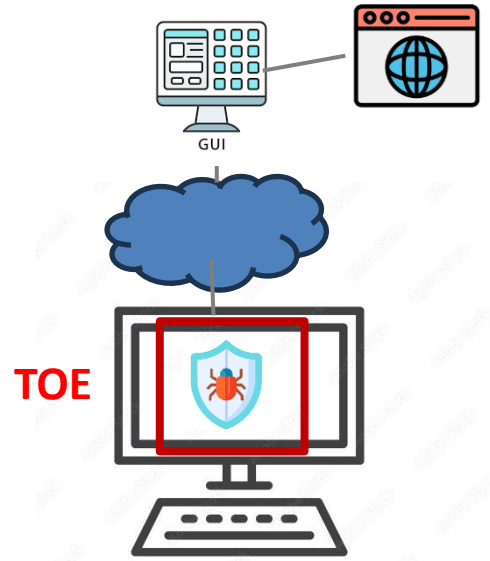
Remote data processing solutions

CRA Recital (11)
The purpose of this Regulation is to ensure a high level of cybersecurity of ***products with digital elements*** *and* ***their integrated remote data processing solutions****. Such remote data processing solutions should be defined as* ***data processing at a distance for which the software is designed and developed*** *by or on behalf of the manufacturer of the product with digital elements concerned,* ***the absence of which would prevent the product with digital elements from performing one of its functions***
[…]
"websites that ***do not support the functionality*** *of a product with digital elements,* ***or cloud services designed and developed outside the responsibility of a manufacturer*** *of a product with digital elements* ***do not fall within the scope of this Regulation****."*

Managed switch remote console



EDR remote dashboard console / update server



The concept might require clarification:

- Example: remote banking/payment infrastructure located on the backend of a payment termina.

EUCC is currently not suitable or optimized to evaluate cloud services.

- ✓ Use alternative cloud-suitable methods to demonstrate CRA conformity of the remote data processing (i.e., future European cloud certification scheme, or harmonized standard)

Closing Gaps Proposal

GAP 1: EUCC certification doesn't cover all CRA ESRs

- ✓ **Add SFRs / SARs to Security Target** for applicable ESRs
- ✓ **Update Security Problem Definition** to justify non-applicability of other ESRS.

GAP 2: Scope of the TOE smaller than scope of the product

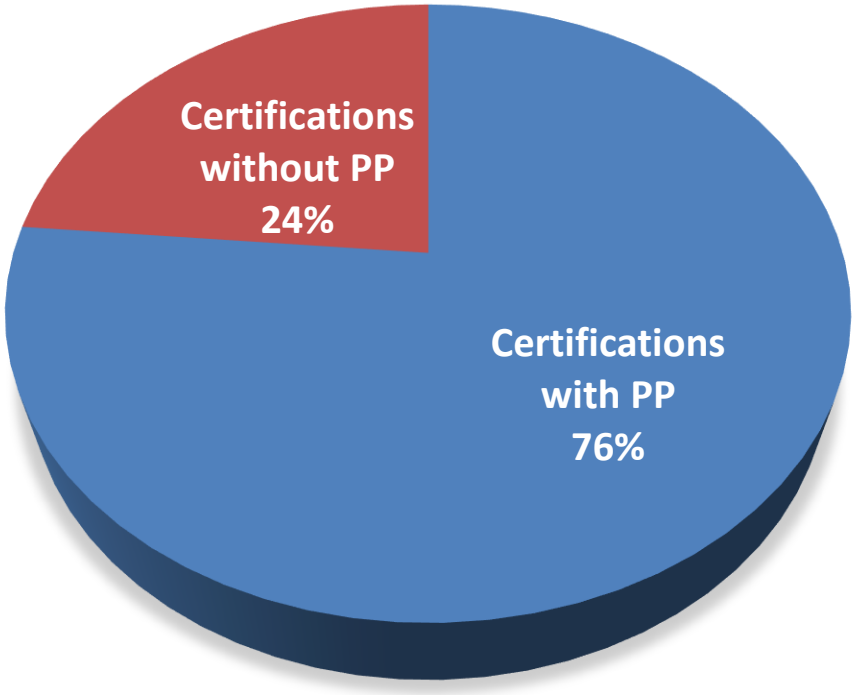
- ✓ **Enlarge TOE scope** (if impact is affordable), or
- ✓ Update **SPD** to **demonstrate that non-TOE parts** of the product are sufficiently **protected by the security functions in the TOE scope**

GAP 3: remote data processing solutions not included in certification

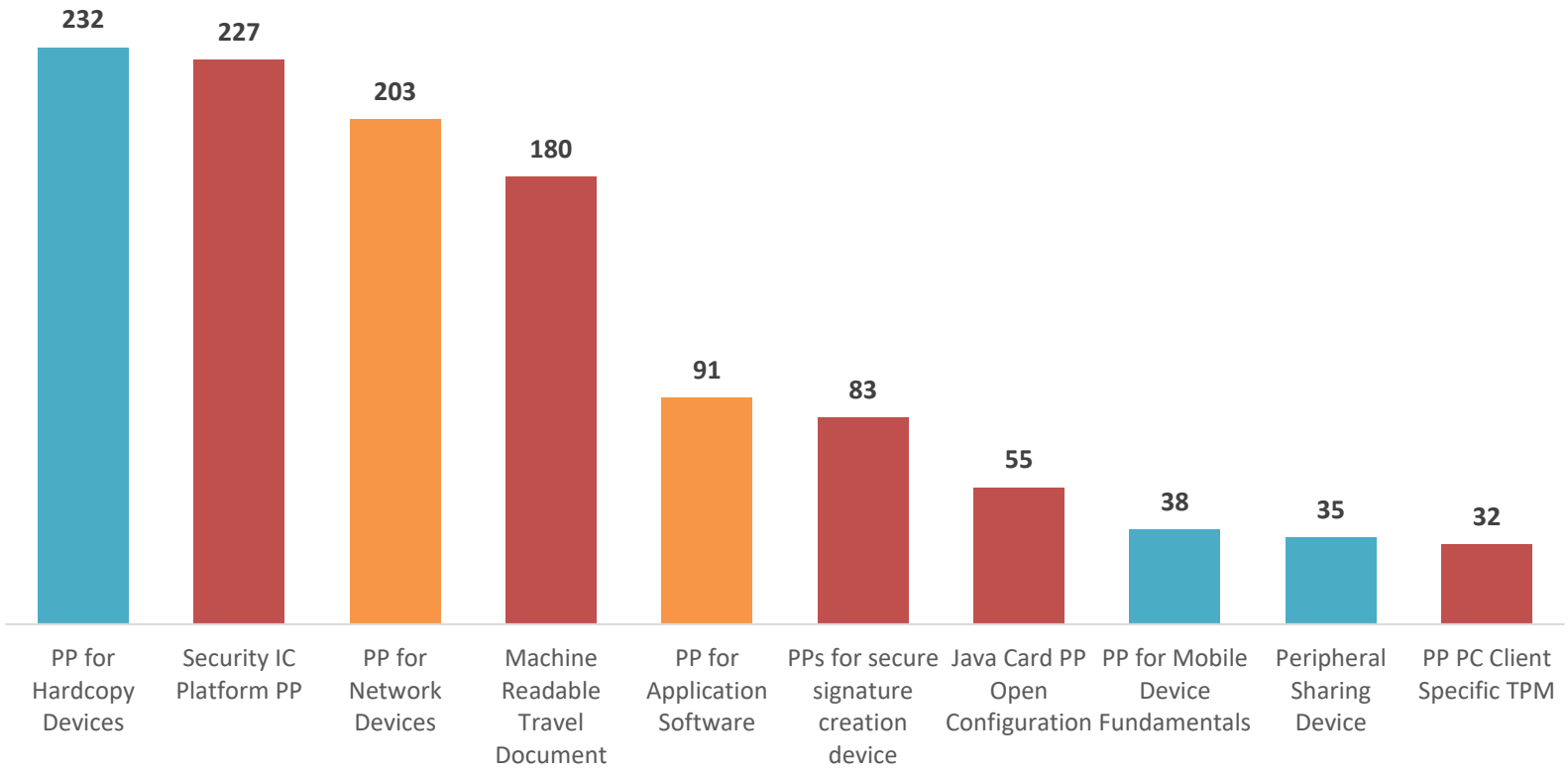
- ✓ Update SPD to include **assumptions on the remote data processing entities**.
- ✓ **Include SFRs protecting communications** with relevant cloud entities.
- ✓ On-cloud entities CRA conformance to be demonstrated through other methods (i.e., harmonized standards)

CC certification industry landscape

CC CERTIFICATIONS (2020 – Oct. 2024)



Top PPs 2020-2024 (October)



- ✓ **Market dominated by Protection Profiles**

Source: jtsec CC statistics

- ✓ **Top-10 PPs are used to certify:**
  - **CRA Critical products: 50%**
  - **CRA Important products: 28%**
  - **CRA non-critical, non-important: 22%**

Gaps in certifications in the industry

Critical products

- Strict or demonstrable conformance (can add SFRs/SARs to existing certifications)
- Scope of the TOE generally matches the full product; No remote data processing
- High assurance, should be possible to demonstrate no further SFRs/SARs are needed

Important products

- Exact conformance frequently used (cannot add SFRs/SARs or modify SPD or scope)
- TOE scope does not always match the full product; On-cloud services often used.
- Potentially should meet additional SFRs/SARs (data minimisation, user data removal…)

Other products

- Diverse scopes and PP conformity. Potentially requiring additional SFRs/SARs
- Not legally obliged, but should take advantage of existing certifications to meet CRA

- Certification of critical products can generally be updated to modify SPD or SFRS/SARs. Existing gaps could be closed through this method.
- Scenarios with **exact conformance** don't allow gap closing updating individual certifications of PP-compliant products (PPs, packages, etc.).
- Certifications of non-important, non-critical products can be updated to close CRA gaps when exact conformance is not used.

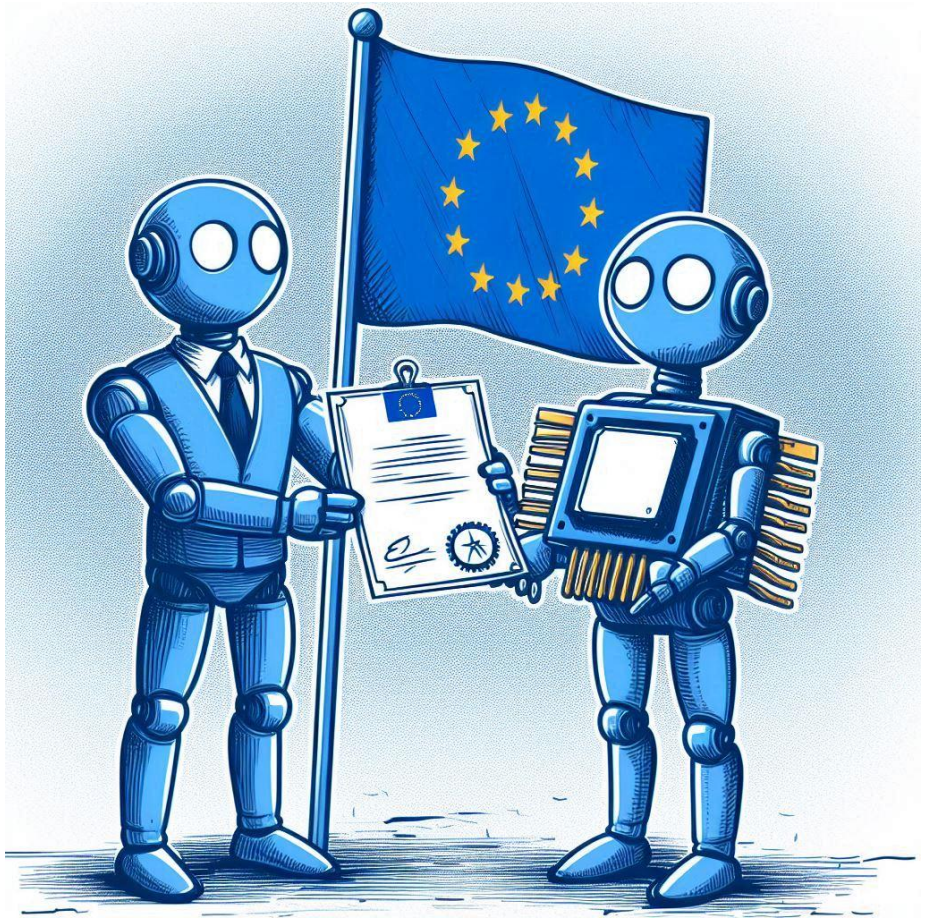
Factors to consider by industry and regulators

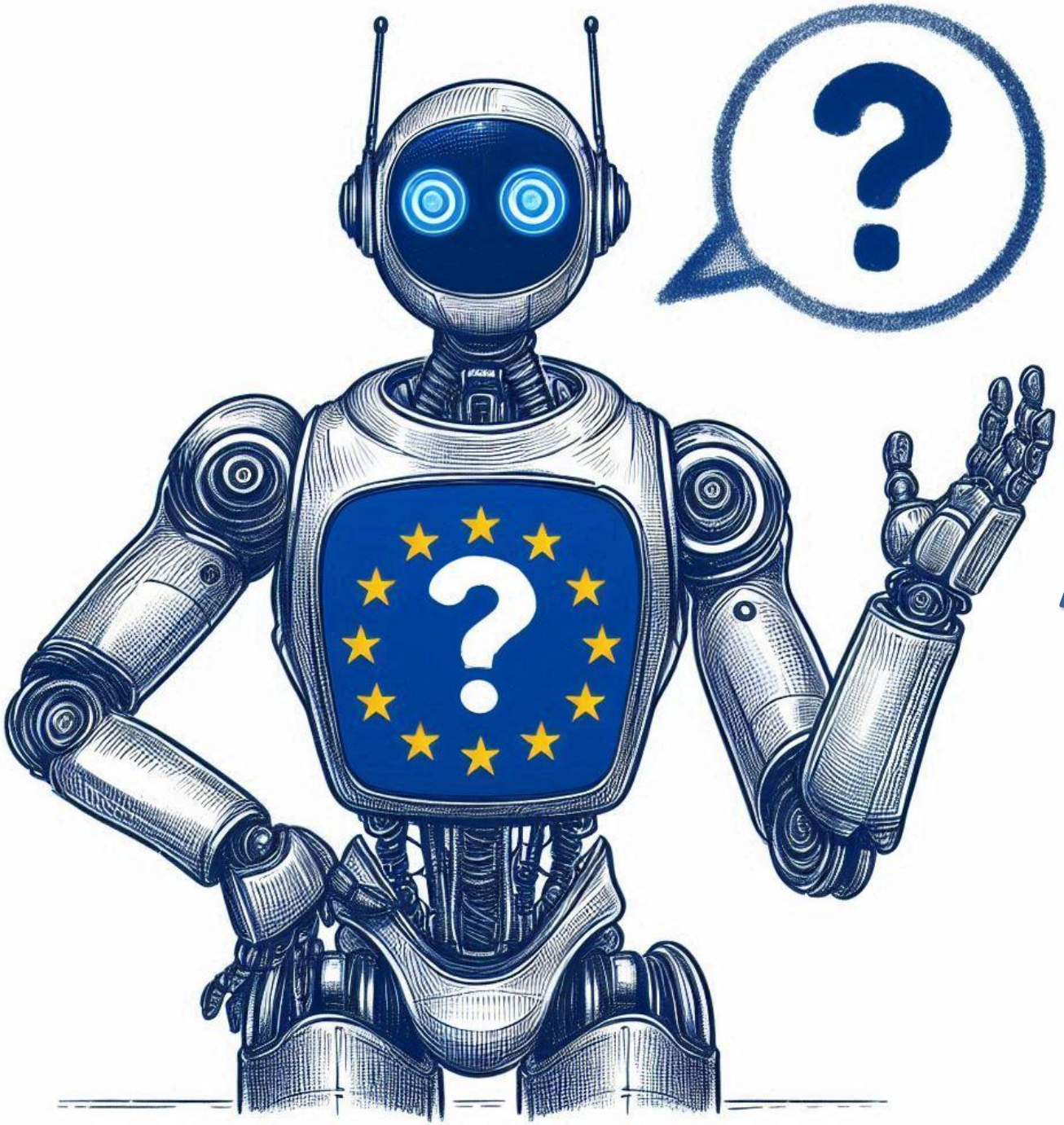
- EUCC brings a **unique opportunity** for the certification industry to meet CRA, **but it is not a universal solution for any product.**

- **PPs are crucial** to introduce CRA compliance (delta) **in a harmonized way in large certification pools.**
  - ✓ **Transition to CC2022:** opportunity to update PPs
  - ✓ **Prioritization** in PPs of products already obligated to certify under EUCC.

- CRA-EUCC interplay should not **change the rules of game** with drastic changes in a mature and well-established industry:
  - ✓ Impact of enlarging TOE scopes.
  - ✓ Impact of additional requirements high assurance technical domains.

- **Non-EU PPs:**
  - Massively used in important products sold in the EU.
  - Exact conformance vs CRA gaps
  - Recognition agreements + CRA delta PP update would solve CRA compliance in already certified products.





Any questions?

Contact

jtsec: Beyond IT Security

Granada & Madrid – Spain

hello@jtsec.es

@jtsecES

www.jtsec.es

"Any fool can make something complicated. It takes a genius to make it simple."
Woody Guthrie