jtsec

Applus

Using EUCC to meet 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.

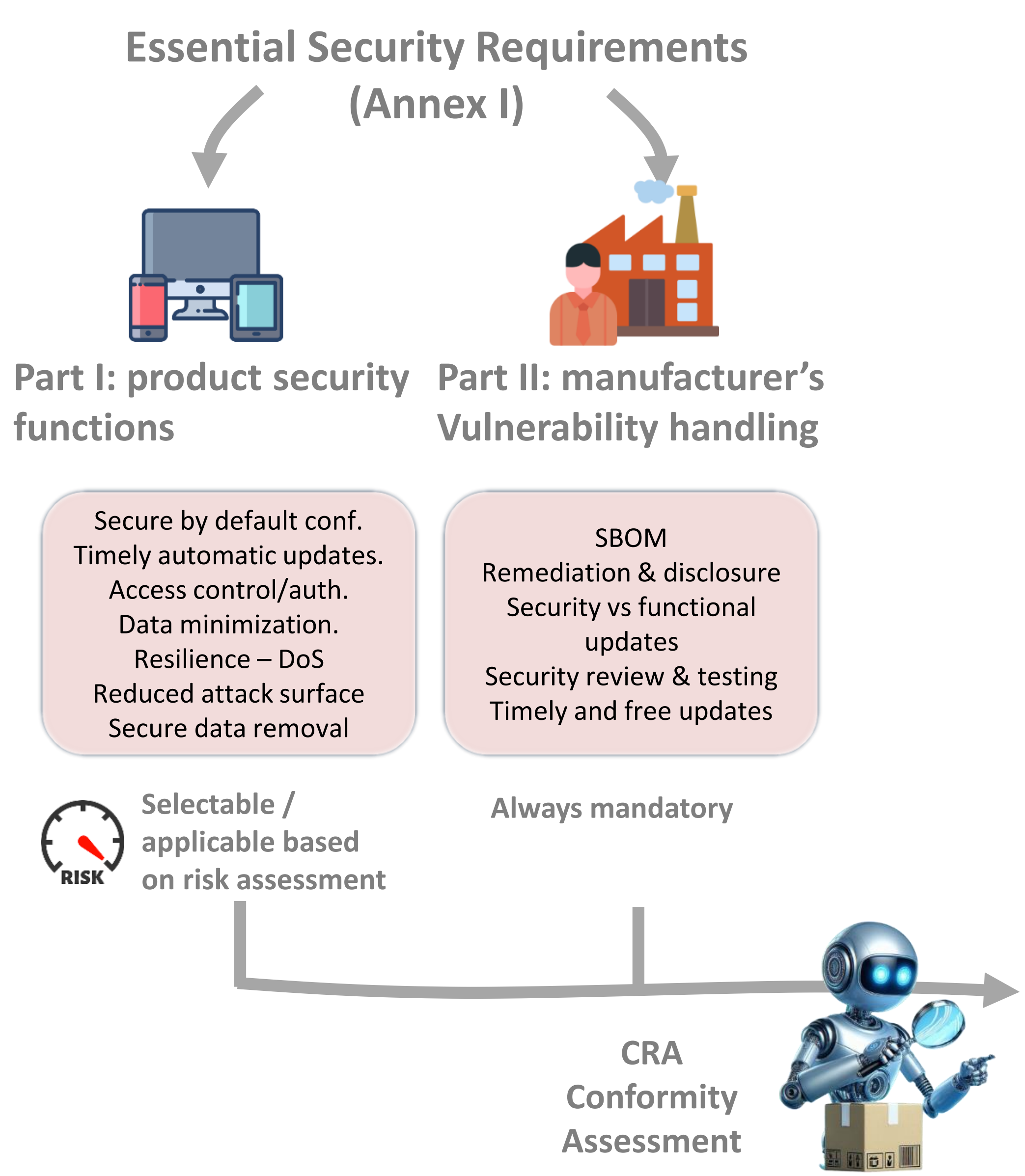
Key obligations for Manufacturers

- 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

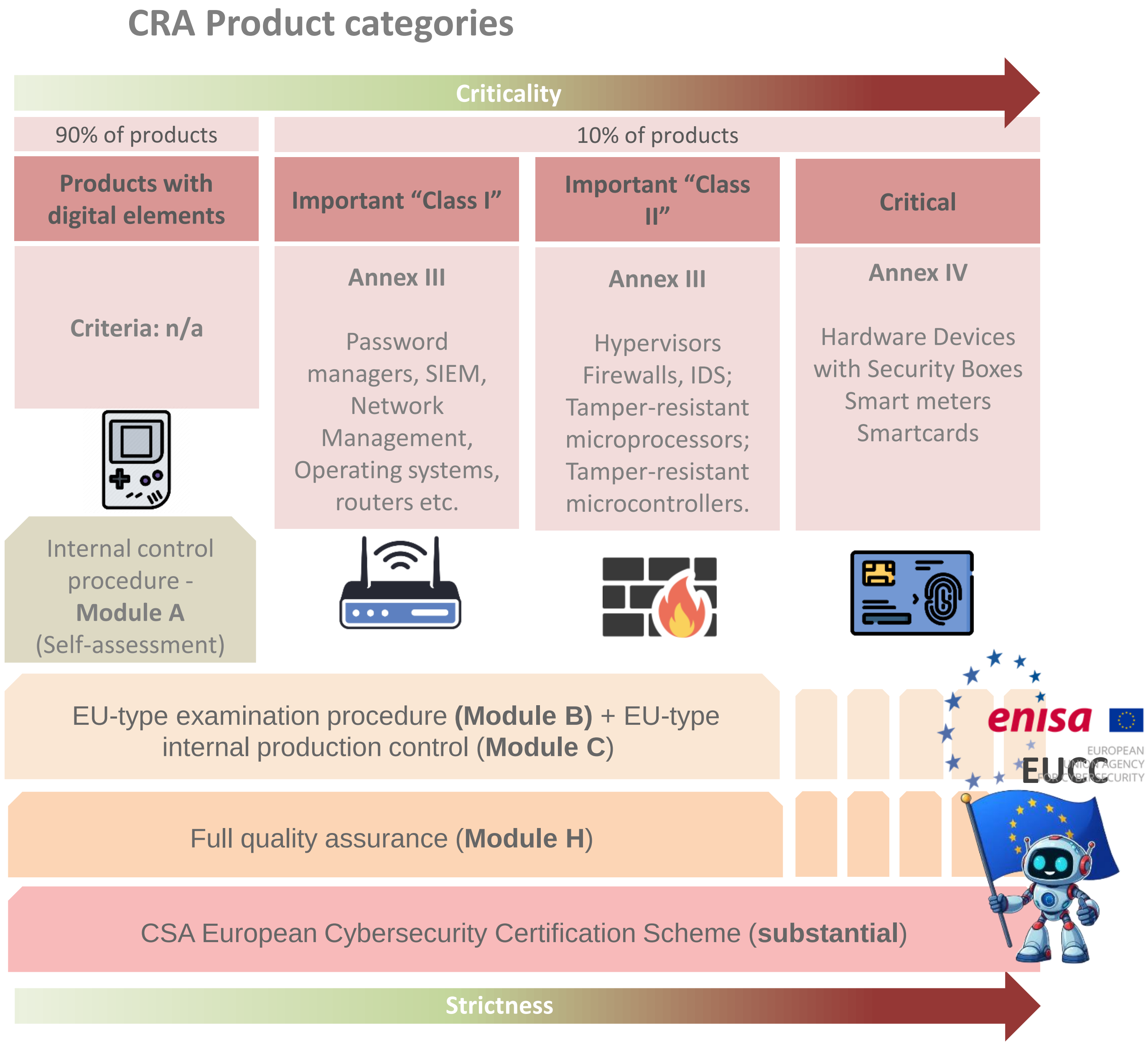
Selectable / applicable based on risk assessment

Part II: manufacturer's Vulnerability handling

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

Always mandatory

CRA Conformity Assessment



CRA Product categories

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

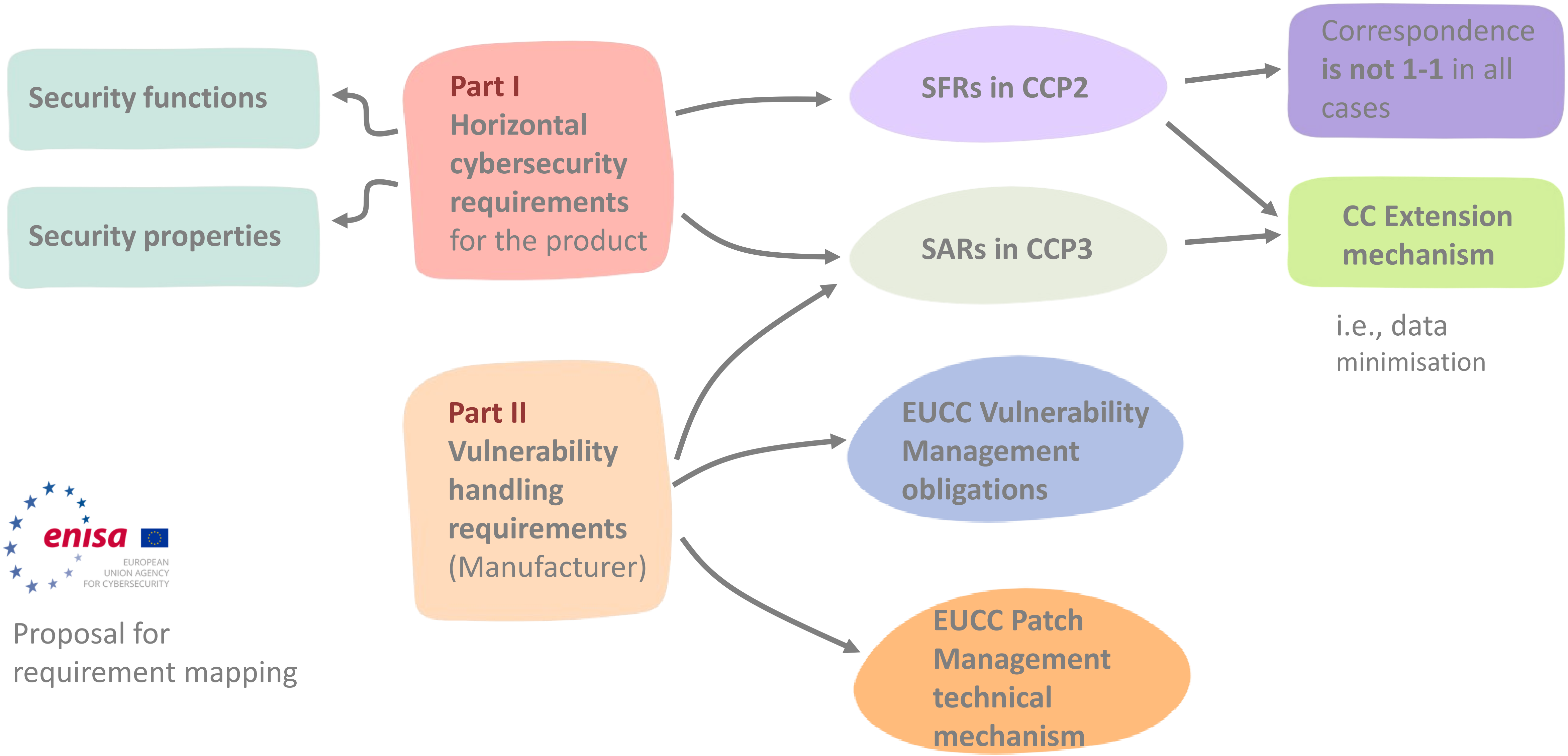
Internal control procedure - **Module A** (Self-assessment)

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

Full quality assurance (**Module H**)

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

CRA ESRs: Annex I Part 2 & EUCC technical elements



Security functions

Security properties

Part I
Horizontal cybersecurity requirements
for the product

Part II
Vulnerability handling requirements
(Manufacturer)

SFRs in CCP2

SARs in CCP3

EUCC Vulnerability Management obligations

EUCC Patch Management technical mechanism

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

CC Extension mechanism

i.e., data minimisation

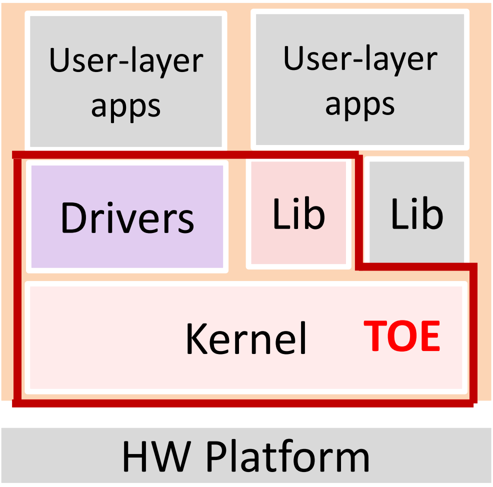
Proposal for requirement mapping

Beyond Essential Security Requirements

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 vs CRA scope:

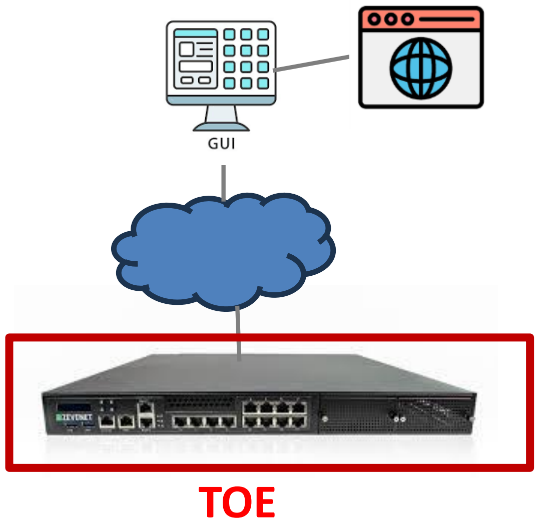
- CC scope is often smaller than the full product
- CRA compliance of TOE parts outside the EUCC scope?
- **Key:** does the in-scope TOE protect the full product? Partial presumption of conformity?



Operating system

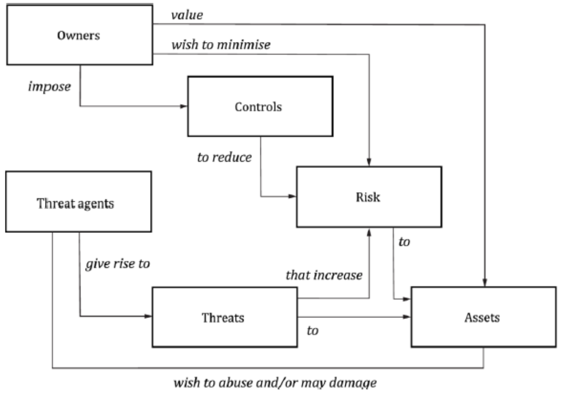
On-cloud non-TOE components:

- EUCC can't always deal and isn't optimized with evaluation of on-cloud components.
- **Key:** demonstration of CRA compliance through other methods (i.e., harmonized standards)



Risk assessment

- CRA article 13 requires a risk assessment leading to applicability of ESRs (Annex I P1)
- **Key:** Security Problem Definition as simplified risk assessment + ASE_REQ + previous risk assessment (CC Part 1)



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)

Gap bridging implementation

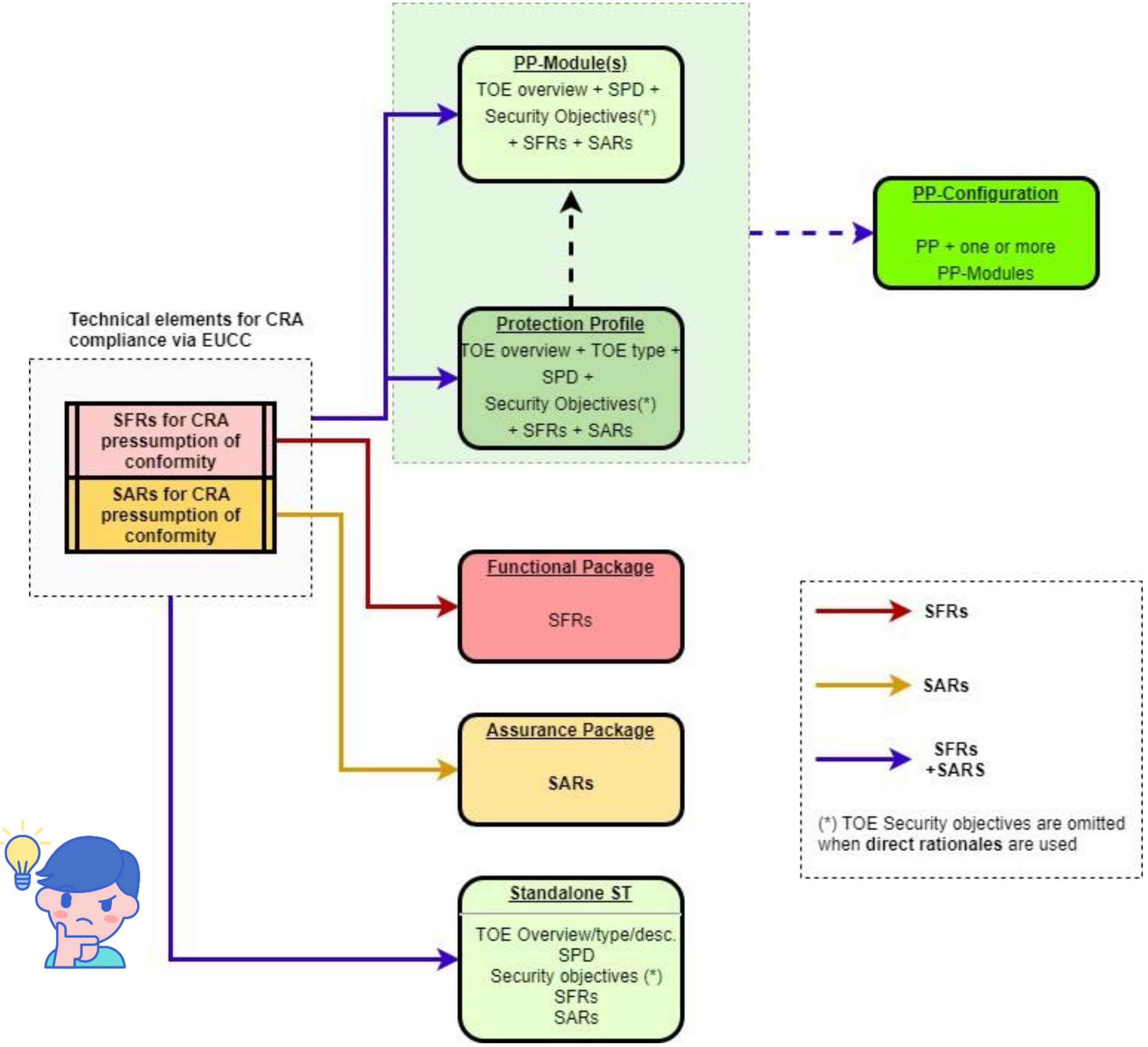
How to implement changes in existing certifications?
(update SFRs, SARs, SPD, scope…)

The chosen mechanisms should provide:

- **Harmonization**, i.e., avoid analysing chosen SFRs/SARs in each certification.
- **Flexibility**: allow inclusion or exclusion of technical elements in different scenarios

Generalist options such as a single CRA-PP might be unpractical, complex and too large. Packages might work better.

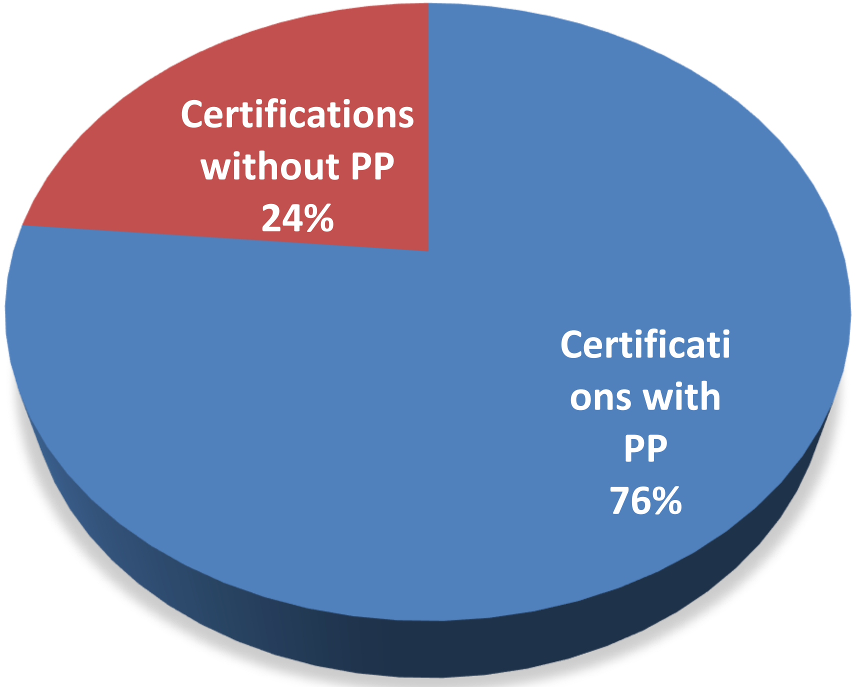
Are these options compatible with the real landscape of the certification industry?



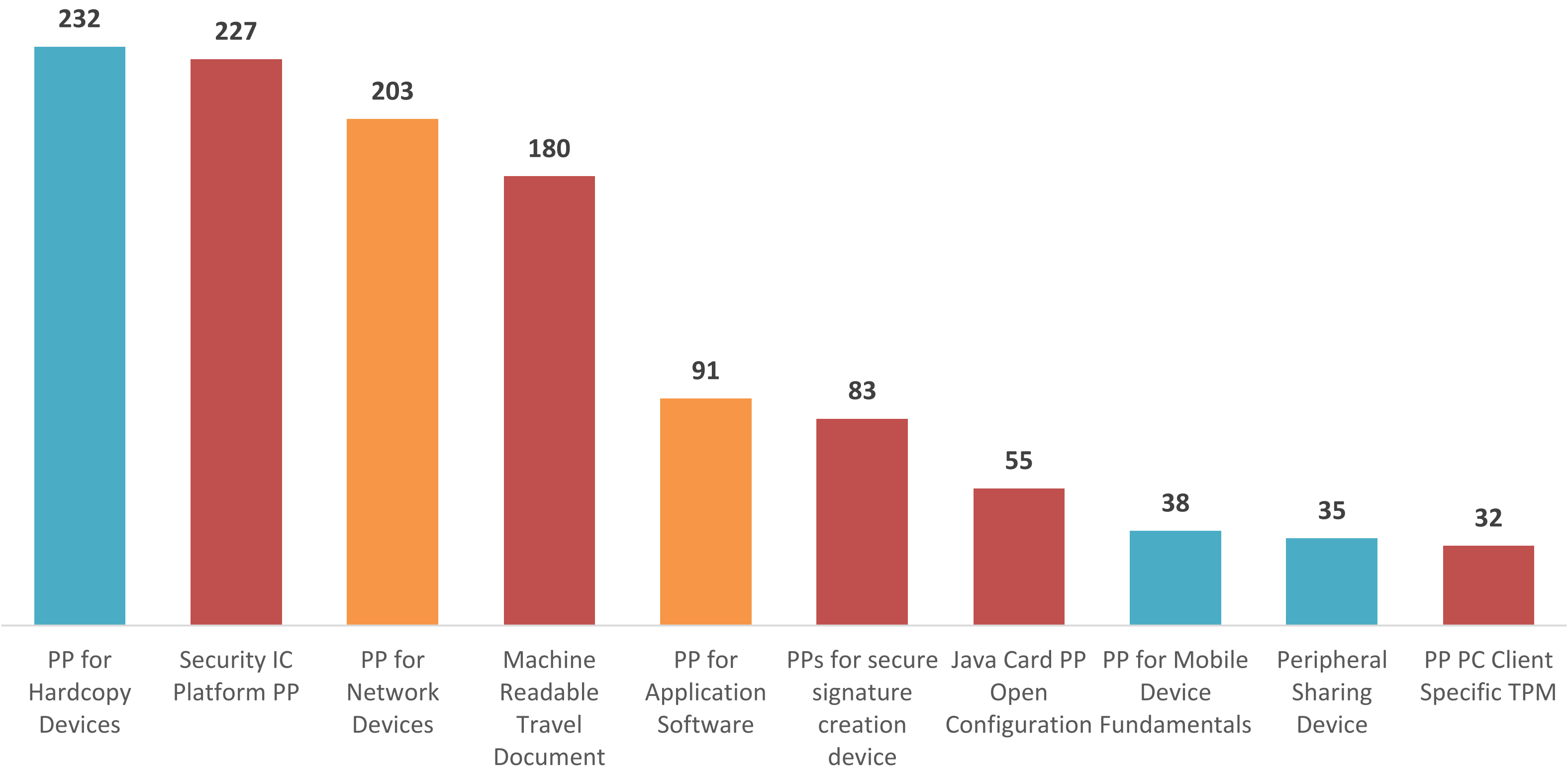
Technical elements for CRA compliance via EUCC
SFRs for CRA pressumption of conformity
SARs for CRA pressumption of conformity
PP-Module(s)
TOE overview + SPD + Security Objectives(*) + SFRs + SARs
Protection Profile
TOE overview + TOE type + SPD + Security Objectives(*) + SFRs + SARs
PP-Configuration
PP + one or more PP-Modules
Functional Package
SFRs
Assurance Package
SARs
Standalone ST
TOE Overview/type/desc.
SPD
Security objectives (*)
SFRs
SARs
SFRs
SARs
SFRs +SARS
(*) TOE Security objectives are omitted when direct rationales are used

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%

Implementation strategy

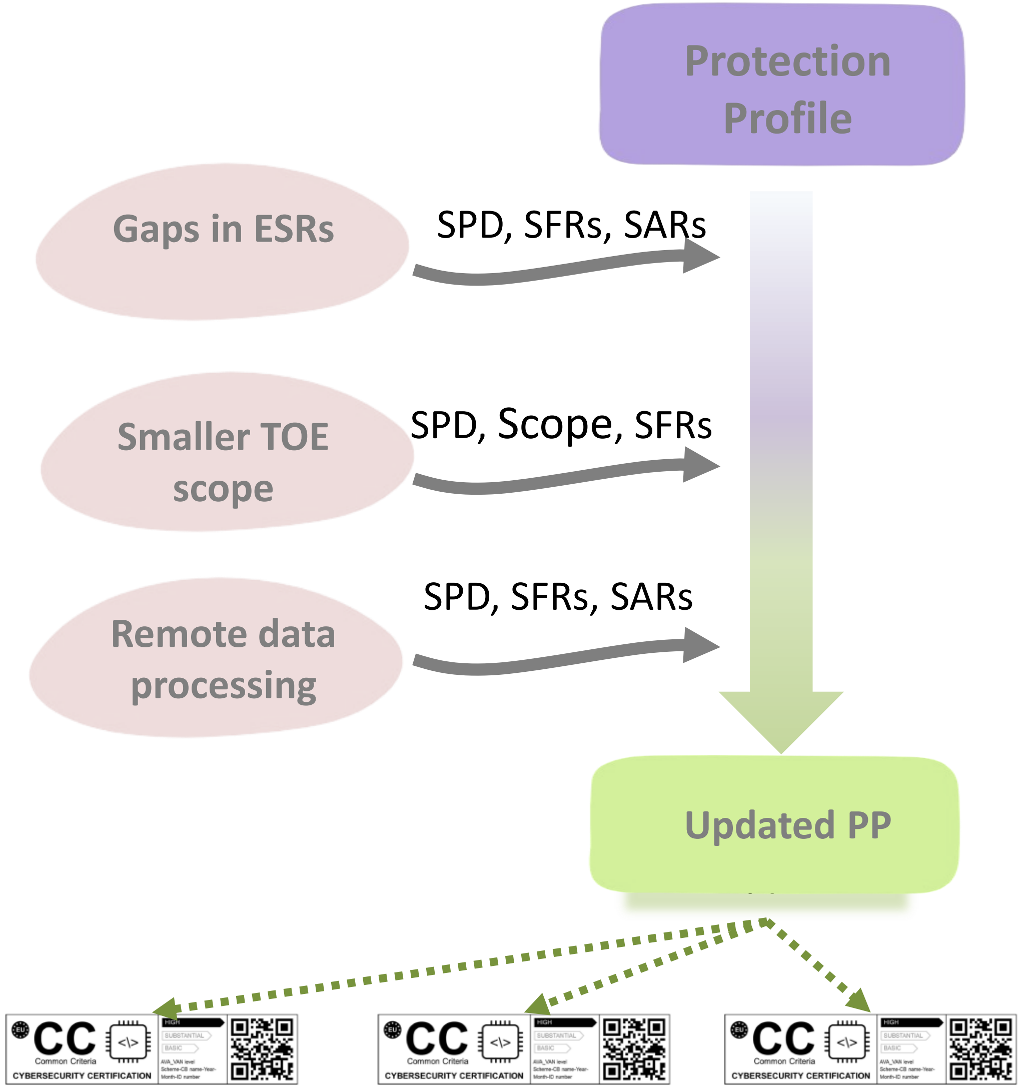
Strategy idea: undertaking gap closing through updating PPs rather than on individual certifications.

- Certification industry dominated by PPs.
- CRA-compliance analysis (risk assessment, SPD, TOE scope, SFRs/SAR) done **once** and by expert technical communities, SDOs or NCCAs.
- Scenarios with **exact conformance** prevent gap closing without updating the PPs.

Prioritizing the update of PPs of products that, for one or other reason, are required to obtain an EUCC certificate.

- Critical product PPs should be quick wins (high-priority).
- EUCC is not cheap, fast or entry-level. It might not be a solution for all manufacturers that need to meet CRA.

When no PPs are used, **functional and assurance packages**, or **modular PPs**, tailored for CRA conformance can be developed.


Protection Profile
Gaps in ESRs
SPD, SFRs, SARs
Smaller TOE scope
SPD, Scope, SFRs
Remote data processing
SPD, SFRs, SARs
Updated PP
CC Common Criteria CYBERSECURITY CERTIFICATION
CC Common Criteria CYBERSECURITY CERTIFICATION
CC Common Criteria CYBERSECURITY CERTIFICATION

PP-compliant certificates meeting CRA

Contact

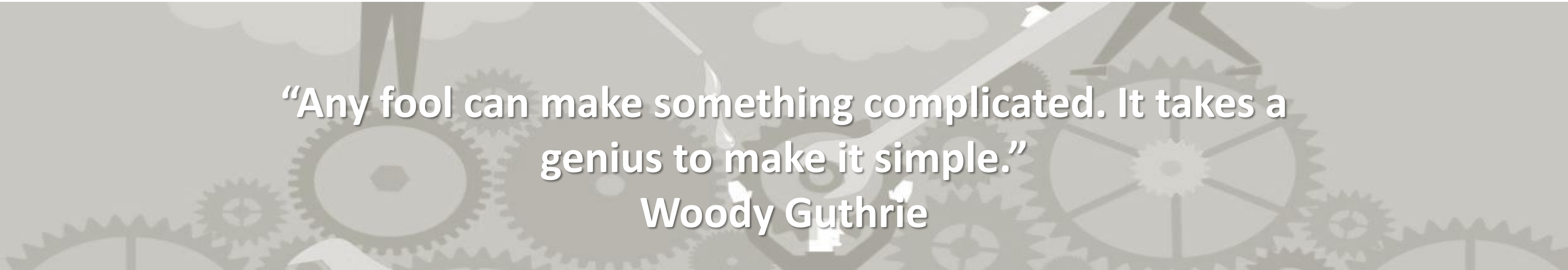
jtsec: Beyond IT Security

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