EUROPEAN UNION AGENCY
FOR CYBERSECURITY

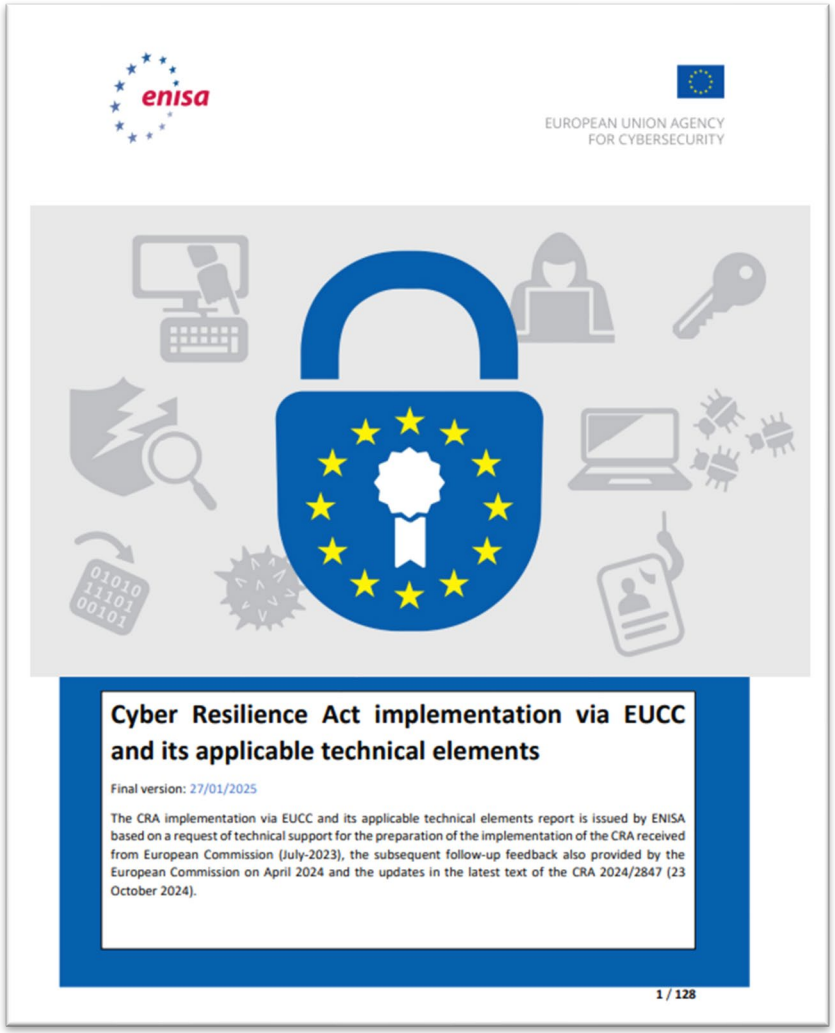
WEBINAR
EUCC CRA INTERPLAY

Vicente Gonzalez Pedros
ENISA Cybersecurity Expert (Cybersecurity Certification Unit)

Jose Manuel Pulido Carrillo
CEI Expert (JTSEC)

2 06 2025

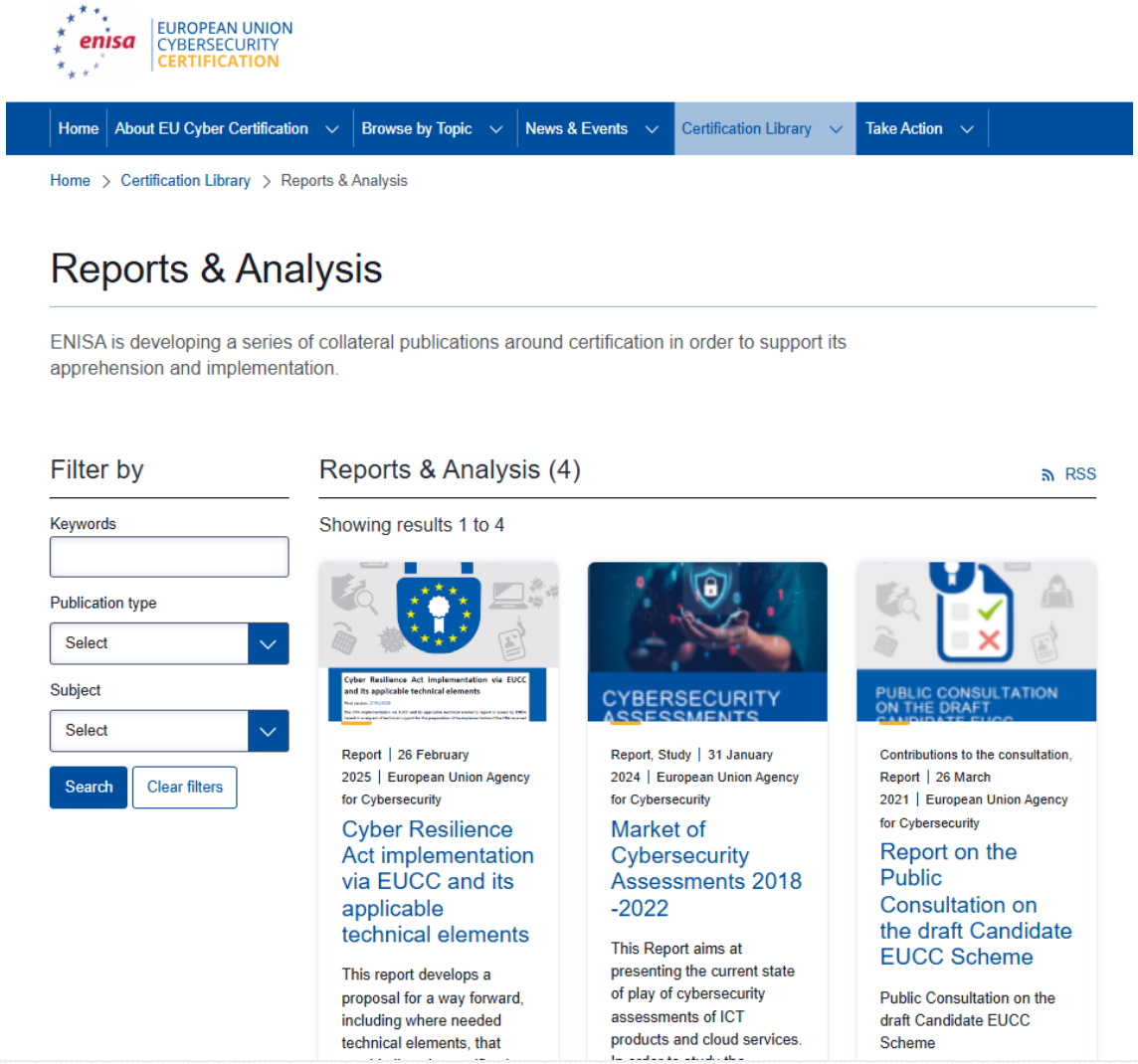
INTRODUCTION TO THE STUDY

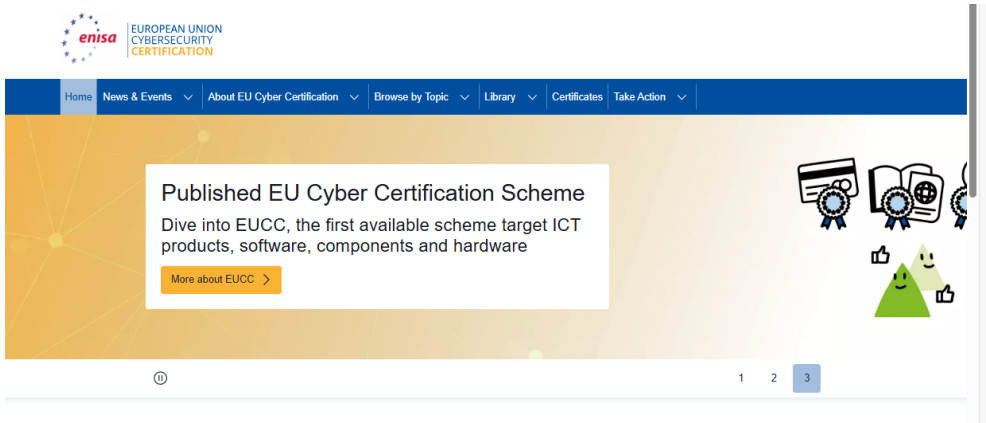


- **July 2023:** Request from the Commission to ENISA
- **Nov 2023:** Nov 2023: First strategy report linking CRA & EUCC, presented at ENISA Certification Week (Málaga).
- **July 2024:** Revised to reflect CRA changes (Mar 2024) & EUCC Implementing Act; shared with ECCG/SCCG.
- **September 2024:** received and applied feedback from stakeholders
- **January 2025:** final version published in ENISA website

Purpose: Initial analysis to guide future use of EUCC to demonstrate CRA compliance.

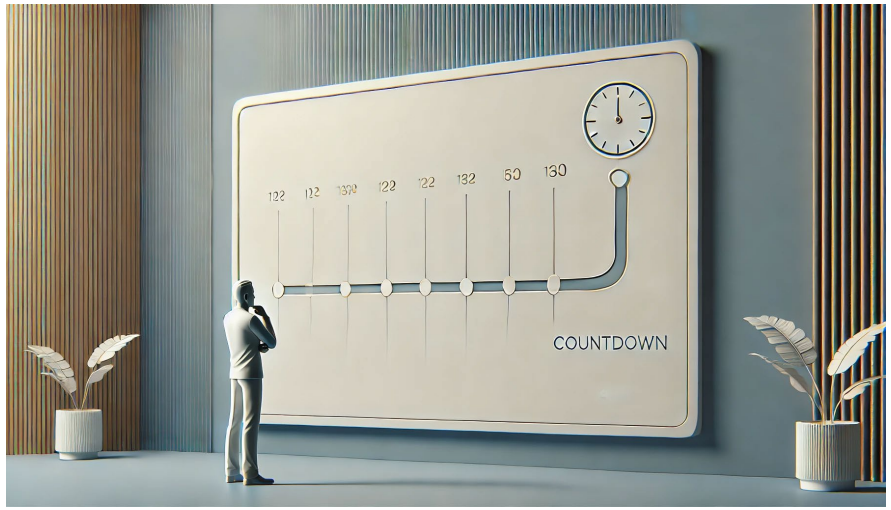
ENISA CERTIFICATION WEBSITE





https://certification.enisa.europa.eu/

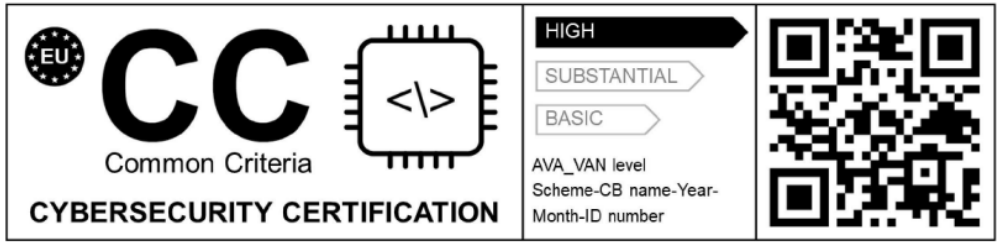
EU Cyber Resilience Act (CRA) - Deadlines



Deadlines

- 27/02/2024 – EUCC Entry into force.
- 11/12/2024 – CRA Entry into force. (20 days)
- 27/02/2025 – **EUCC into application.**
- 11/09/2026 – Notification provisions to the CSIRT and ENISA. (21 Month)

- 31/12/2027 – End of use of CC 3.1 in EUCC
- January 2028 – CRA into Application (36 Months).



Strategies for implementation in the industry

Timelines for updates of Protection Profiles

1. CC v3.1 R5 is the last revision of version 3.1 and may optionally be used for evaluations of Products and Protection Profiles starting no later than the 30th of June 2024.

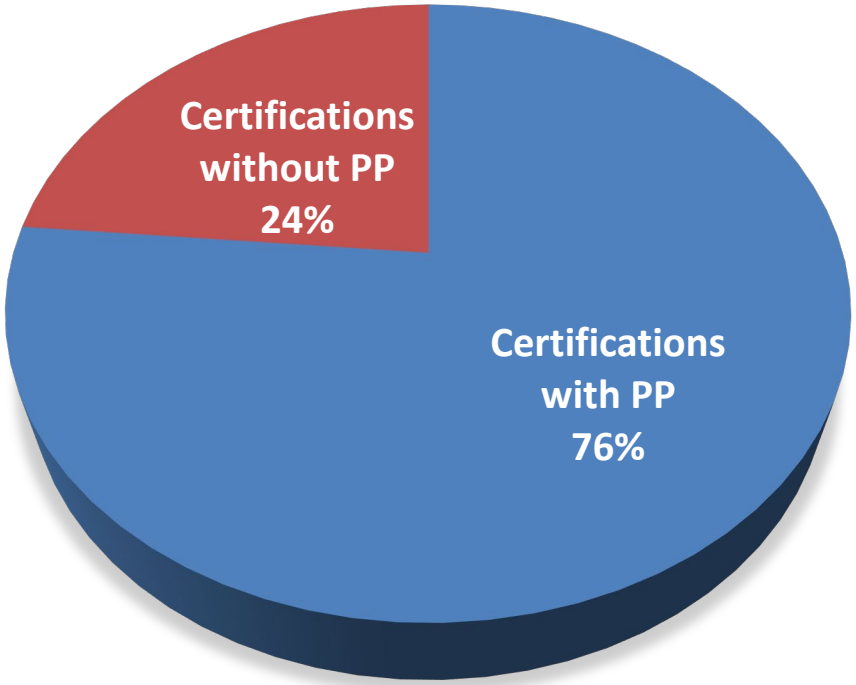
2. Security Targets conformant to CC:2022 and based on Protection Profiles certified according to CC v3.1 ***will be accepted up to the 31st of December 2027.***

3. After 30th of June 2024, re-evaluations and re-assessments based on CC v3.1 evaluations can be started for up to 2 years from the initial certification date.

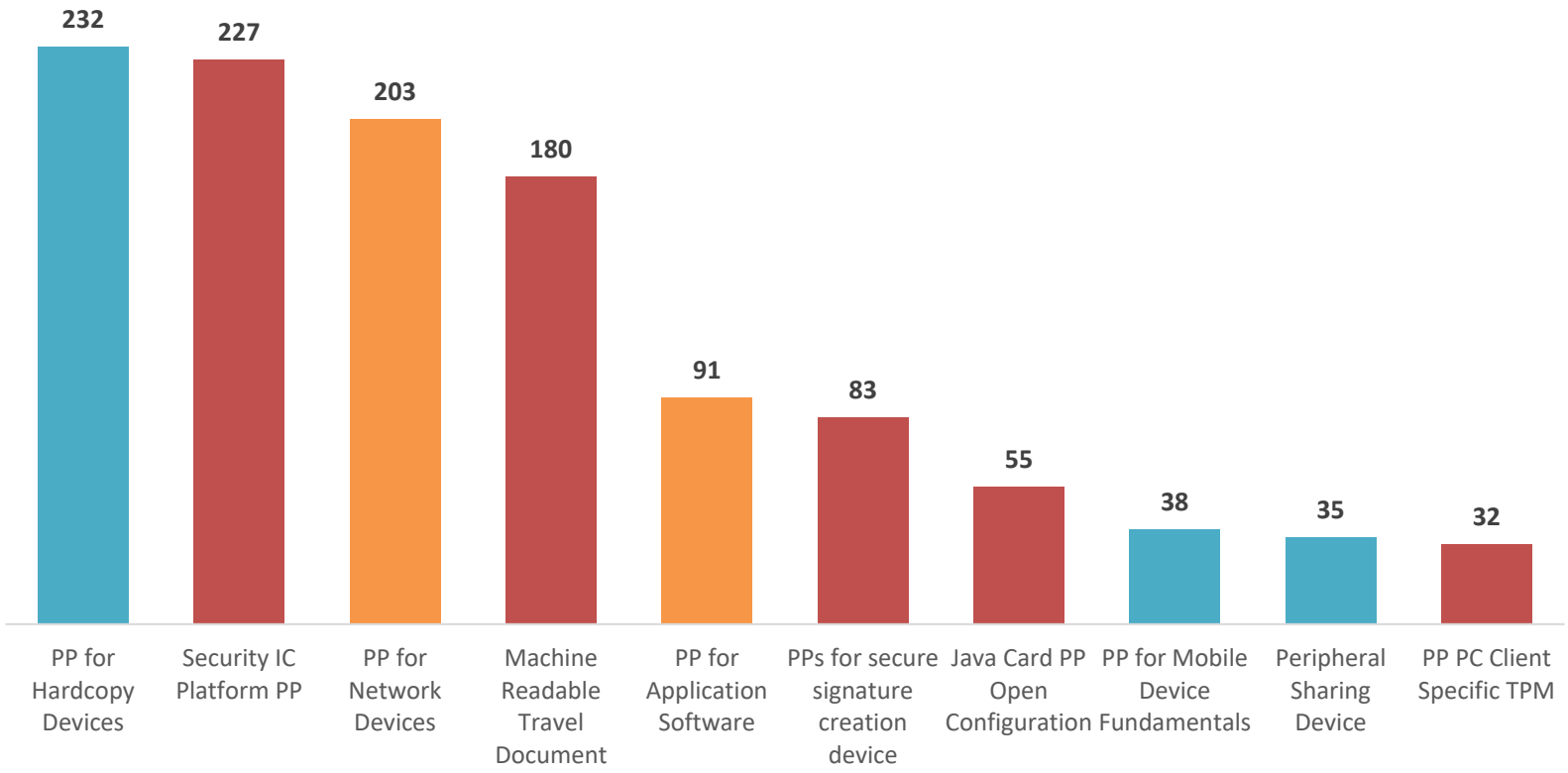
According to point 2 above, the use of protection profiles written using CC v3.1 R5 in Security Targets will be disallowed after 2027. Therefore, existing PPs based on that version of CC shall be updated to CC2022 before that date.

Use of Protection Profiles in CC Industry

CC CERTIFICATIONS (2020 – Oct. 2024)



Top PPs 2020-2024 (October)



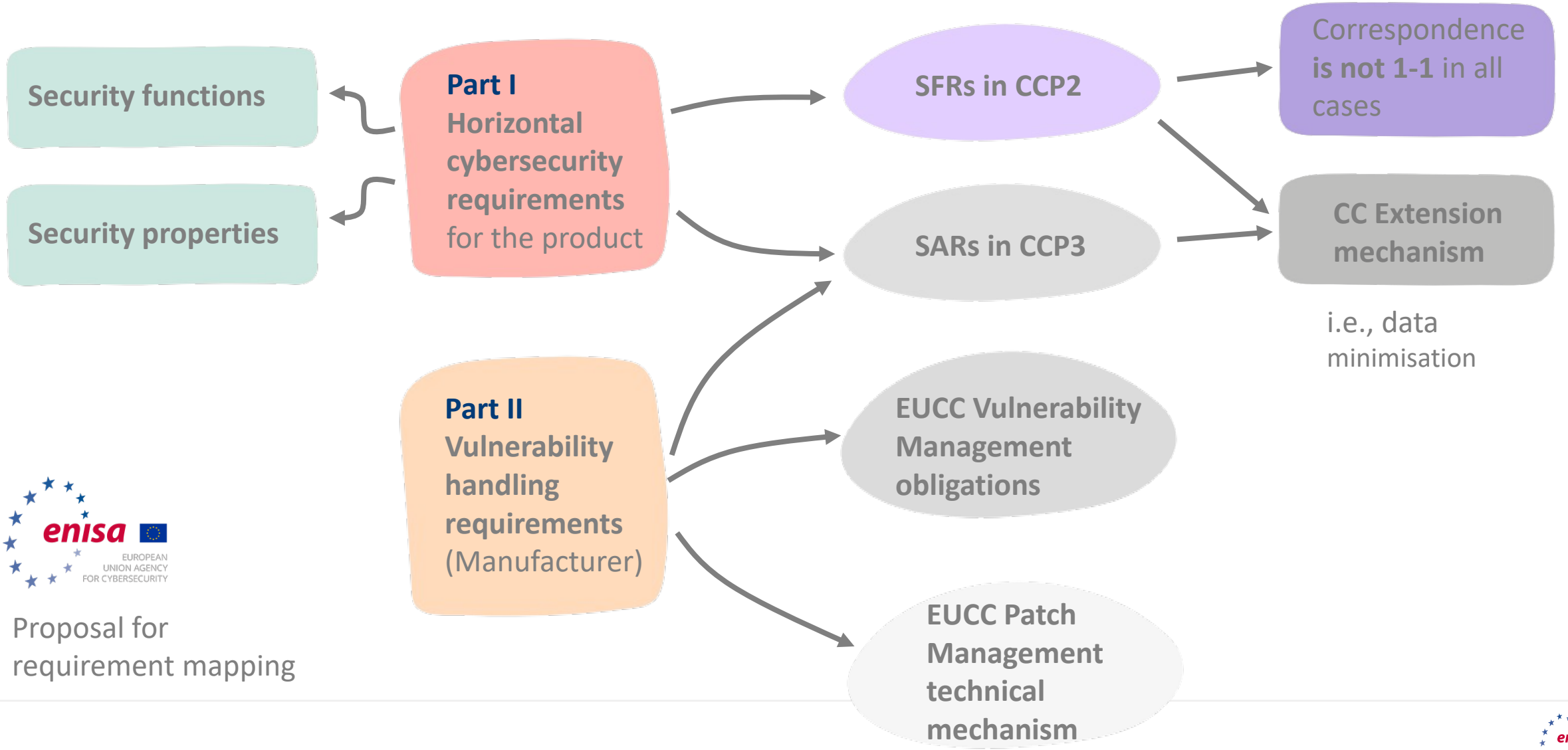
- ✓ **Market dominated by Protection Profiles**
- ✓ **Top-10 PPs are used to certify:**
  - **CRA Critical products: 50%**
  - **CRA Important products: 28%**
  - **CRA non-critical, non-important: 22%**

Source: jtsec CC statistics

EUCC CABs alignment with NBs under CRA

- Under the Cybersecurity Act (CSA), EUCC CABs must be accredited and, for level High, authorised by national authorities (Art. 61 CSA), and notified to the Commission.
- Under the Cyber Resilience Act (CRA), notification does not require accreditation, but CABs must comply with Art. 39 CRA and demonstrate this to the notifying authority.
- A comparison performed in the study shows strong alignment between EUCC CAB requirements (CSA Annex) and CRA Art. 39, particularly regarding:
  - ✓ Legal status & independence
  - ✓ Impartiality & liability
  - ✓ Technical competence & procedures
  - ✓ Confidentiality & transparency
- ISO/IEC 17065 supports both schemes; EUCC CABs already assessed under it are well positioned.
- **Dual role possible**: EUCC CABs could *potentially* act as CRA Notified Bodies — especially useful to assess overlaps, e.g., CC Protection Profiles vs CRA Essential Requirements.
- **Conclusion:** With minor adjustments, EUCC CABs could qualify as CRA Notified Bodies, fostering synergies across EU cybersecurity frameworks

CRA ESRs mapping to EUCC Technical elements



enisa
EUROPEAN UNION AGENCY FOR CYBERSECURITY

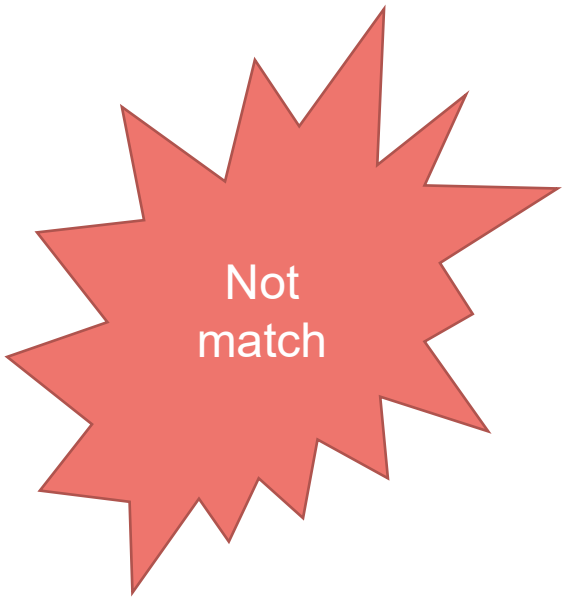
Proposal for requirement mapping

CRA ESRs mapping to EUCC Technical elements

Essential security requirement (CRA Annex I, Part I)	CC SFRs (from [CC2022P2] or extended)	CC SARs (from [CC2022P3] or extended)	Notes
(1) *Products with digital elements shall be designed, developed and produced in such a way that they ensure an appropriate level of cybersecurity based on the risks;*		ASE_SPD.1 Security problem definition ASE_OBJ.1 Security objectives ASE_REQ.1 Direct rationale security requirements	The Security Problem Definition is based on a risk analysis that ultimately leads in CC to selection of SFRs and SARs that can define security aspects equivalent to those in CRA ESRs. It is done in a way similar than that in CRA, where the manufacturer's risk assessment leads to the selection of applicable ESRs from those in CRA Annex I, part 1.
(2) *On the basis of the cybersecurity risk assessment referred to in Article 13(2) and where applicable, products with digital elements shall:*	-	-	-
(2)(a) *be made available on the market without known exploitable vulnerabilities;*		AVA_VAN.1 Vulnerability survey	Any EUCC evaluation with assurance level "substantial" or "high" may directly fulfil this requirement.
(2)(b) be *made available on the market with a secure by default configuration, unless otherwise agreed between manufacturer and business user in relation to a tailor-made product with digital elements, including the possibility to reset the product to its original state;*	FMT_SMF.1 Specification of Management Functions	ADV_ARC.2 Security Architecture with Default Secure Configuration (Extended)	FMT_SMF.1 shall include a management function that permits resetting the TOE to its initial or default configuration. Other SFRs or SARs with equivalent functionality could also meet the requirements, the ones given here are merely one proposal. Alternatively, ADV_ARC.2 could be left out of the evaluation if: a) An agreement as mentioned in the ESR is provided with the technical documentation. b) The risk assessment contemplates a compensating security measure making the requirement not applicable or necessary. A practical

CRA ESRs mapping to EUCC Technical elements

Essential security requirement (CRA Annex I, Part I)	CC SFRs (from [CC2022P2] or extended)	CC SARs (from [CC2022P3] or extended)	Notes
(1) *Products with digital elements shall be designed, developed and produced in such a way that they ensure an appropriate level of cybersecurity based on the risks;*		ASE_SPD.1 Security problem definition ASE_OBJ.1 Security objectives ASE_REQ.1 Direct rationale security requirements	The Security Problem Definition is based on a risk analysis that ultimately leads in CC to selection of SFRs and SARs that can define security aspects equivalent to those in CRA ESRs. It is done in a way similar than that in CRA, where the manufacturer's risk assessment leads to the selection of applicable ESRs from those in CRA Annex I, part 1.
(2) *On the basis of the cybersecurity risk assessment referred to in Article 13(2) and where applicable, products with digital elements shall:*	-	-	-
(2)(a) *be made available on the market without known exploitable vulnerabilities;*		AVA_VAN.1 Vulnerability survey	Any EUCC evaluation with assurance level "substantial" or "high" may directly fulfil this requirement.
(2)(b) be *made available on the market with a secure by default configuration, unless otherwise agreed between manufacturer and business user in relation to a tailor-made product with digital elements, including the possibility to reset the product to its original state;*	FMT_SMF.1 Specification of Management Functions	ADV_ARC.2 Security Architecture with Default Secure Configuration (Extended)	FMT_SMF.1 shall include a management function that permits resetting the TOE to its initial or default configuration. Other SFRs or SARs with equivalent functionality could also meet the requirements, the ones given here are merely one proposal. Alternatively, ADV_ARC.2 could be left out of the evaluation if: a) An agreement as mentioned in the ESR is provided with the technical documentation. b) The risk assessment contemplates a compensating security measure making the requirement not applicable or necessary. A practical

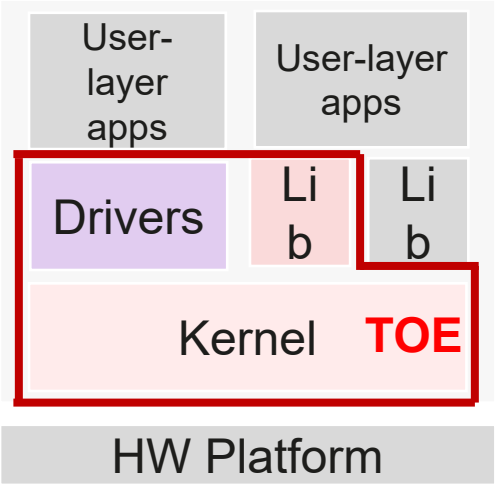


Beyond Essential Security Requirements

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

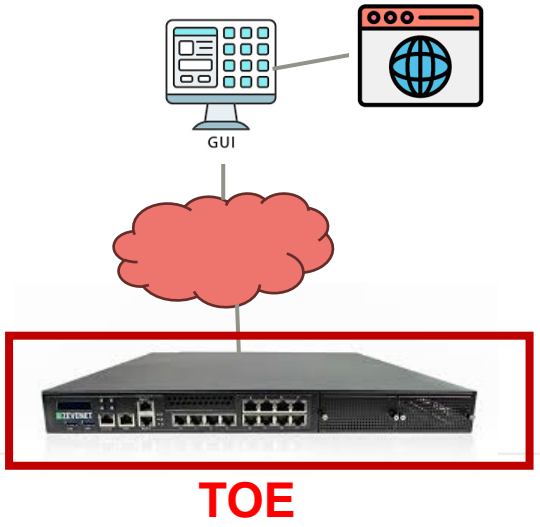
CC TOE scope vs CRA scope:

- 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?



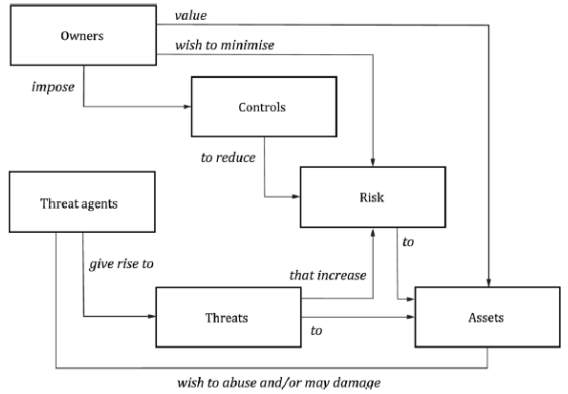
On-cloud non-TOE components:

- 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

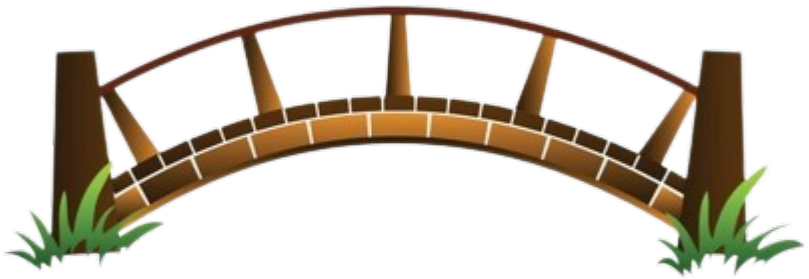
- CRA article 13 requires a risk assessment leading to applicability of ESRs (Annex I P1)
- **Key:** Security Problem Definition as simplified risk assessment + ASE_REQ + previous risk assessment (CC Part 1)



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)

PPs as vehicular tool for implementation

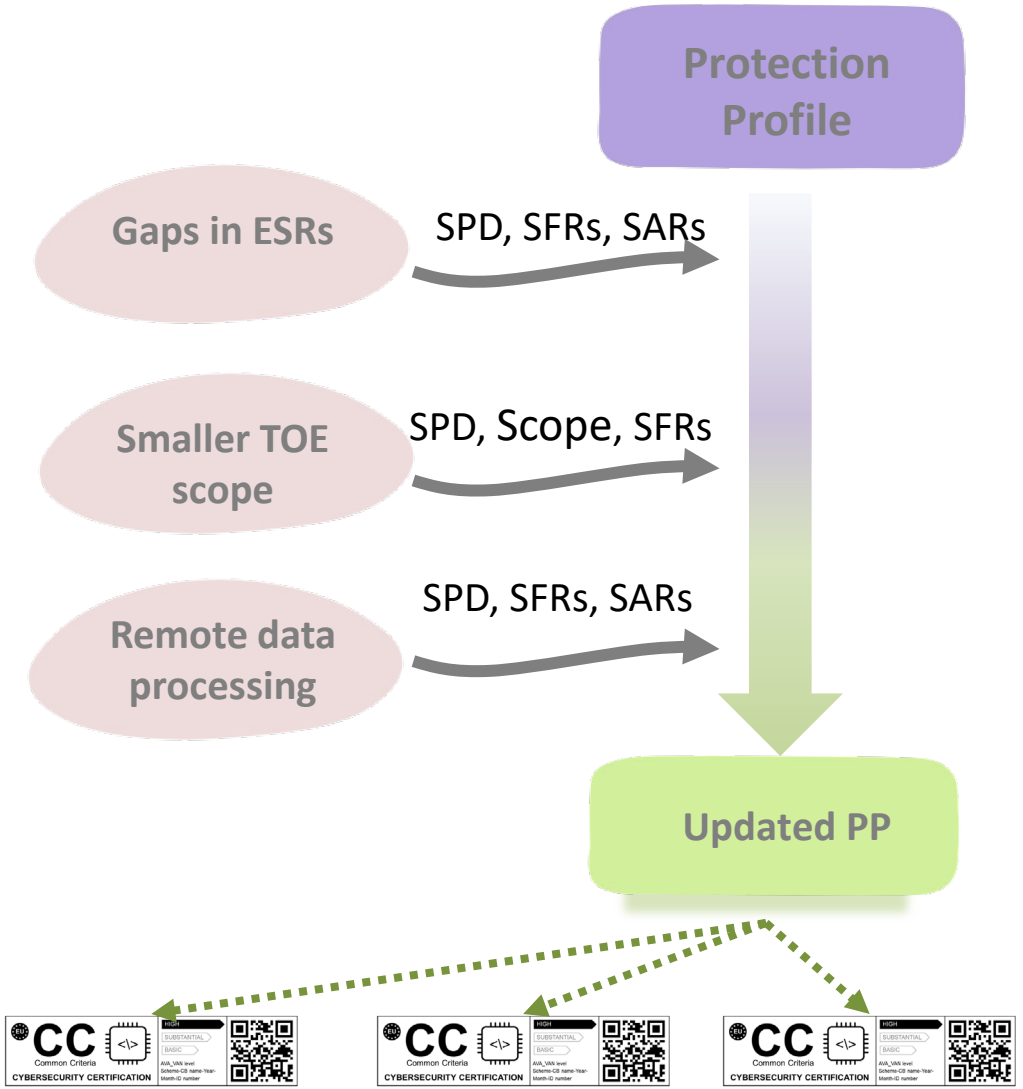
Strategy idea: undertaking gap closing through updating PPs rather than on individual certifications.

- 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.



PP-compliant certificates meeting CRA

PILOTS

Pilots:

- ✓ **10 Pilots** at lest two of them for non PP certification.
- ✓ Engage with international community to collaborate in the update of the PP and cPP.

Objectives :

- ✓ **Update PP for CRA Compliance.**
- ✓ **Propose a Generic PP for CRA compliance.**
- ✓ **Update the Study** as a guidance for PP updates.

PILOTS ROADMAP