ENISA - Support to Pilot the EUCC CRA Interplay

CALL FOR INTEREST

ENISA - European Union Agency for Cybersecurity
Ethnikis Antistaseos 72 & Agamemnonos 14, Chalandri
15231, Attiki - Greece

TABLE OF CONTENTS

1 INTRODUCTION

The European Union has reinforced its approach to cybersecurity regulation with the Cyber Resilience Act (CRA), formally Regulation (EU) 2024/2847, which introduces essential cybersecurity requirements (ESRs) for products with digital elements. In parallel, the EU Common Criteria-based certification scheme (EUCC), adopted via Commission Implementing Regulation (EU) 2024/482 under the Cybersecurity Act (Regulation (EU) 2019/881), offers a structured pathway for product certification aligned with internationally recognised standards.

ENISA, in collaboration with the European Commission and relevant stakeholders, has already published a technical study on the interplay between EUCC and CRA. This study proposes the use of EUCC to demonstrate conformity with CRA ESRs, including detailed mappings of security requirements and extended components. To validate these proposals, pilot evaluations are now planned for selected Protection Profiles and for certifications that don't use a PP. These pilots aim to test the technical feasibility and practical application of the proposed mappings and assurance elements.

The study can be found on the ENISA Certification website. EUCC CRA Interplay

The results of these pilots will provide potential updates of the EUCC–CRA interplay study, as well as guidance for its application.

1.1 ABOUT THE PROJECT

The CRA recognises EUCC as a key tool to demonstrate compliance with its ESRs, especially for digital products falling within the scope of critical and important product categories. As such, ENISA's pilot project is instrumental in validating the CRA–EUCC interplay and refining technical mappings, new modules to complement EUCC, and templates of Manufacturer declarations that may be needed like the free security updates.

This call for pilots aims to support the validation of the EUCC–CRA interplay study through manufacturer/ITSEF/CBs/CABs collaboration, providing several activities mentioned below. It operates at a high strategic and technical level to ensure a harmonized and actionable pathway to CRA compliance.

It is recommended to review the webinar done by ENISA and European Commission to present the project. The webinar can be found at ENISA Certification Website.
Webinar EUCC CRA Interplay

1.2 OBJECTIVES

The main objectives of the Pilots are to:

1. Test the EUCC–CRA Interplay: Determine whether and how the current EUCC framework provides a viable and effective path to demonstrate compliance with the Cyber Resilience Act (CRA). This includes assessing whether the alignment proposed in the existing EUCC–CRA Interplay study is functional in practice.

2. Identify Gaps and Adjustments: Where alignment gaps are identified, gather evidence and feedback to specify what adjustments—whether technical, procedural, or regulatory—are needed to ensure the EUCC may support CRA conformity.

3. Validate Technical Mappings and Workflow: Use pilot evaluations to test and refine the technical mappings between CRA Essential Security Requirements (ESRs) and the Security Functional Requirements (SFRs) and Security Assurance Requirements (SARs) within the EUCC, and assess whether the needed SFRs and SARs should/could be added to existing PPs, remain isolated, or gathered as an optional PP module. Adjust the certification workflow as needed based on practical insights.

4. Inform ENISA to Update the EUCC–CRA Interplay Report: ENISA will consolidate the pilot results and stakeholders' outputs into an updated version of the EUCC–CRA Interplay Report, including proposals for future implementation. This updated version will become a Guidance to be followed for the update of PPs or for certifications without PPs.

5. Provide ENISA with any additional recommendations for the CRA compliance using EUCC Certification, including complementing EUCC with NLF relevant modules. Such recommendations could present the expected characteristics of such modules when combined with the certification of products.

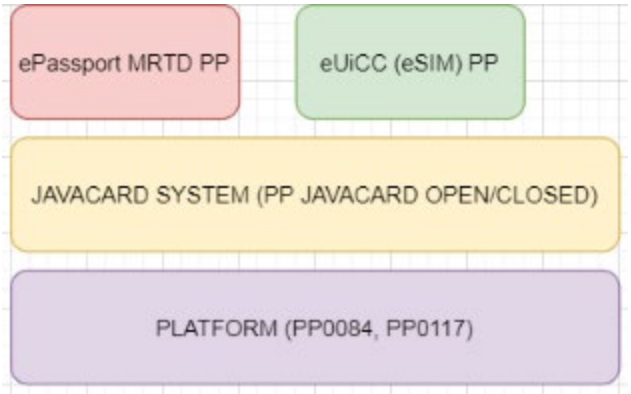
1.3 PILOT CALL

ENISA invites participation from the following actors involved in EUCC certification:

- Conformity Assessment Bodies (CABs), including:
  - Certification Bodies (CBs)
  - Information Technology Security Evaluation Facilities (ITSEFs)
- Manufacturers of products with digital elements
- Industry Alliances, European and International Organisations with a relevant mandate.

Pilots may be composed of one or more stakeholders and are expected to address complete evaluation workflows. Given interdependencies between Protection Profiles, coordination across pilots may be required.

Example: For a composite product requiring multiple PPs (see example below), the respective pilot teams should coordinate to align on common ESR interpretations and shared evidence for the different layers composing the final product.



2 CONFIDENTIALITY AND LEGAL CONSIDERATIONS

All information exchanged within the scope of a pilot will be treated as confidential, and pilot participants will be required to sign a non-disclosure agreement.

Deliverables or data submitted will remain the intellectual property of the respective contributor unless otherwise agreed, but will have to be made available to ENISA and its contractor(s) to gather individual results and to allow establishing a consolidated report.

3 PLAN

The timelines for these pilots are determined as followed.

Applications for pilots are open until 25th of August.

Once ENISA confirms the validity of a proposed a pilot, online meetings on alignment will be organised individually for each pilot: two in August and one every week in September.

Also, a collaborative space for open discussion in a restricted community (only Pilots and related teams' members) will be available for the project.

A hybrid workshop to align and validate the first results is planned on a one and a half day on the 6th of October and the next morning.

- August 2025: up to two preparatory online meetings
- September 2025: Weekly alignment online meetings
- October 6-7, 2025: Hybrid workshop (one-and-a-half-day session)
- More coordination meetings may be organized to validate the final outcomes on early Q1 2026.
- Continuous: Secure collaborative workspace provided by ENISA

Additional waves of pilot projects may be considered in the following months.

4 EXPECTED OUTCOMES

Main activities to be accomplished by the pilot are described below.

DETERMINE CRA COMPATIBLE TOE

Objective: Define the Target of Evaluation (TOE) to align Common Criteria (CC) scope with CRA scope.

Pilot Team Activities:

- Analyze the system/product architecture to identify the components that constitute the **TOE**.
- Determine which elements of the TOE fall under the CRA scope (i.e., digital products, software elements, connected components).
- Map CC boundaries to CRA obligations to ensure clarity on what is being evaluated.
- Prepare documentation describing the **TOE**, including interaction between subsystems and external dependencies.
- Define assumptions, usage environment, and critical assets.

RISK ASSESSMENT (CRA ART. 13)

Objective: Identify relevant Essential Security Requirements (ESRs) based on risk.

Pilot Team Activities:

- Conduct a **CRA-aligned risk assessment**, particularly focusing on Article 13 of the Cyber Resilience Act.
- Identify threats and vulnerabilities relevant to the composite TOE.
- Evaluate risks based on likelihood and impact, using standard methodologies.
- Determine which ESRs from the CRA are applicable to the TOE and which are not. Provide a rationale (justification) for excluding specific ESRs from further consideration.
- A template will be delivered to document the information by the PMO.

SECURITY PROBLEM DEFINITION

Objective: Analyse and update if needed the Security Problem Definition (SPD) and Security Objectives for the TOE and its environment.

Pilot Team Activities:

- Analyse and update if needed the **Security Problem Definition (SPD)**, identifying threats, assumptions, organizational security policies, and assets to be protected.
- Based on the SPD, define the **Security Objectives** for the TOE and its operational environment.
- Ensure that the security objectives cover the applicable CRA ESRs identified during the risk assessment.
- Determine the assurance level for the TOE. Analyze where possible a multi assurance approach.

- Align the CC-oriented security objectives with CRA compliance needs.

Record and structure these elements to serve as a basis for defining Security Functional Requirements (SFRs).

MATCHING ESR (CRA) WITH SFRS AND SARS (EUCC)

Objective: Ensure CRA ESRs are covered by CC Security Functional and Assurance Requirements.

Pilot Team Activities:

- Identify the **SFRs and SARs** relevant to the TOE.
- Map each ESR from CRA to:
  - SFRs (e.g., from Part 2 of CC, ISO/IEC 15408)
  - SARs (e.g., from Part 3 of CC, Evaluation Assurance Levels)
- Determine if the ESRs are already covered by selected SFRs/SARs or if **GAPs** exist.
- For uncovered ESRs, propose additional SFRs/SARs or note where CRA imposes complementary controls outside the CC domain. Propose if needed templates to document this mapping in a **traceability matrix** showing ESR–SFR–SAR relationships.
  - Propose optional Module with the group of SFRs and SARs for the CRA compliance.
  - Propose a generic PP for the CRA compliance.

Other activities related to ensure consistency of pilot's outcomes:

WORKSHOP ALIGNMENT

Objective: Reach consensus and update EUCC–CRA interplay based on outcomes.

Joint Activities by ENISA, and Pilot Teams:

- Present and discuss results of previous phases, especially:
  - TOE definition
  - ESR applicability and rationale
  - SPD/SOD alignment
  - ESR–SFR/SAR mapping and GAP analysis
- Identify areas where adjustments or clarifications are needed to update the **CRA–EUCC Interplay methodology**.
- Propose on harmonised templates, procedures, and evidence expectations for future conformity assessments.
- Finalise next steps, including revision of templates and pilot feedback reports.

ENISA will organise the necessary meetings with experts to define or extend the PPs and their interconnections with CRA ESR.

FINAL OUTCOME

Each pilot team will be responsible for submitting:

- Initial pilot plan
- Mid-term progress summary
- Final technical report with mapping evidence and recommendations.

A consolidated report will be established by ENISA with the support of its contractor(s) to gather the outcome of the different pilots and identify common conclusions as well as specific ones.

5 PROCESS OF THE PILOTS

The call for interest is open until 25th of August and finalised application forms need to be sent to ENISA by that date.

The execution of the pilots is expected to take place until Q1 2026. Later closure of pilots may be accepted by ENISA if duly justified and beneficial for related pilot projects.

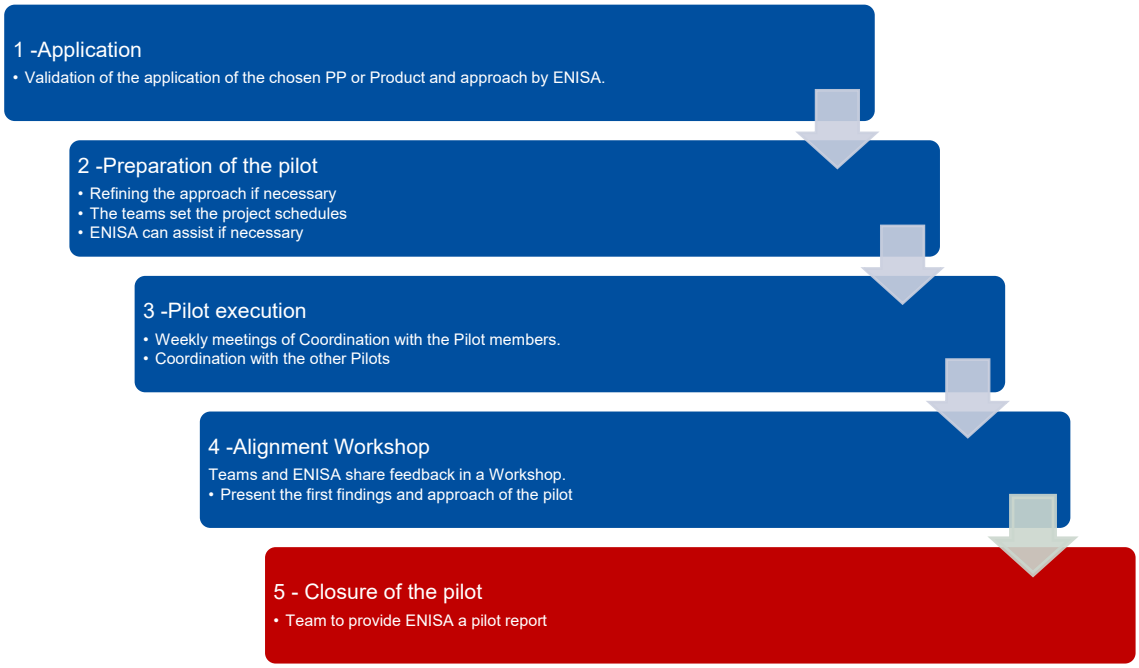
ENISA will accompany each voluntary team in the **step 1 Application** to help define the PP or product if necessary and to make sure different teams have a complementary coverage of the available PP to be updated, even if some redundancy may be accepted as to multiply the experiences.

During **step 2 Preparation** of the pilot, ENISA can provide support in developing the approach.

During **step 3 pilot, ENISA** will coordinate the feedback between the different pilots.

Step 4 – **Alignment workshop**. Feedback to the **pilot's workgroup** at the workshop allow to present the first findings and approach of the pilot. ENISA may invite other participants to this feedback presentation, especially to share the information with developers of the harmonized Standards, EUCC/CRA experts or relevant stakeholders

Step 5 - Closure of the pilot, the teams will provide ENISA with a report with the EXPECTED outcomes.
Where a team asks for it at the application, ENISA may fund these deliverables, if funds are available, description at POTENTIAL FUNDING SUPPORT.



Step 6 – Consilidation of pilots. ENISA wil establish a final report consolidating the outcome and conclusions/recommendations of the different pilots.

6 HOW TO APPLY

Interested parties may apply via the dedicated EU Survey form:

https://ec.europa.eu/eusurvey/runner/Call_for_EUCC_CRA_Interplay_Pilots

Please include:

- Organisational profile and EUCC/CRA experience
- Proposed product or PP area
- Stakeholders involved

Deadline for applications: 25th of August 2025 at 23:59 CEST.

7 SELECTION CRITERIA

ENISA will coordinate the selection of pilot proposals based on the following criteria, as mandated by the European Commission and guided by strategic, technical, and policy considerations under the Cyber Resilience Act (CRA) and the EUCC framework.

STRATEGIC PRIORITISATION BY MARKET IMPACT

Priority will be given to pilot proposals involving Protection Profiles (PPs) that are:

- Widely used in the EUCC certification landscape (based on current certification volume),
- Associated with products listed in CRA Annex III (Important) or Annex IV (Critical) categories,
- Impactful across multiple sectors (e.g., energy, digital infrastructure, industrial control systems).

Target: At least 8 pilots covering the most-used Protection Profiles.

INCLUSION OF NON-PP-BASED CERTIFICATIONS

To address gaps where no PP currently exists, ENISA will prioritise pilot submissions that:

- Involve EUCC certifications conducted solely under a Security Target (ST),
- Aim to propose generic reusable modules (CRA-specific PPs or SAR/SFR packages),
- Demonstrate a cross-cutting relevance to future CRA-compliant certification use cases.

TECHNICAL AND ORGANISATIONAL READINESS

Proposals must demonstrate the ability to carry out technical mapping of ESRs to SFRs/SARs, and include:

- Named technical experts (manufacturer or ITSEF),
- Access to documentation and evaluation artefacts of the certified product,
- Defined roles and timelines aligned with the pilot plan.

BALANCED REPRESENTATION OF STAKEHOLDER ROLES

Preference will be given to pilot teams that include collaboration among:

- Conformity Assessment Bodies (CABs), including:
  - Certification Bodies (CBs)
  - Information Technology Security Evaluation Facilities (ITSEFs)
- Manufacturers of products with digital elements
- National Cybersecurity Certification Authority (NCCA).
- Industry Alliances, European and International Organisations with a relevant mandate.

CONTRIBUTION TO GUIDANCE AND HARMONISATION

Selection will favor proposals that:

- Are willing to contribute templates, feedback, and lessons learned,
- Commit to participate in alignment workshops,
- Propose generic methodologies or reusable mappings that can inform EUCC guidance updates.

GEOGRAPHIC AND SECTORAL BALANCE (SECONDARY CRITERION)

Where feasible, ENISA will ensure a balanced representation of EU Member States and certification ecosystems.

8 POTENTIAL FUNDING SUPPORT

ENISA is currently in the process of establishing a Contribution Agreement with the European Commission, under which financial support for pilot activities may be provided through the Digital Europe Programme (DEP). At this stage, funding is not yet confirmed.

ENISA informs applicants that, should funding become available, financial support may be offered in accordance with the following conditions:

- Eligibility restriction: Legal entities established in associated countries and legal entities established in the Union but controlled from third countries shall not be eligible to participate in tenders linked to this Contribution Agreement, pursuant to the application of Article 12(5) of the DEP Regulation in the context of the 2023–2024 Digital Europe Work Programme.
- Compliance with applicable conditions for service contracts under the Digital Europe Programme.

- Adherence to the principles of transparency, non-discrimination, equal treatment, and sound financial management.

If funding is confirmed, ENISA will communicate specific instructions, eligibility conditions, and the modalities for financial support directly to selected pilot participants.

9 CONCLUSION

This call for pilots provides a strategic opportunity for stakeholders to contribute to the refinement of the CRA-EUCC conformity pathway. The results will support the European Commission and ENISA in establishing practical and harmonised tools for demonstrating cybersecurity compliance across the Union under the CRA framework.