EUROPEAN UNION AGENCY
FOR CYBERSECURITY

Cyber Resilience Act implementation via EUCC and its applicable technical elements

Final version: 27/01/2025

The CRA implementation via EUCC and its applicable technical elements report is issued by ENISA based on a request of technical support for the preparation of the implementation of the CRA received from European Commission (July-2023), the subsequent follow-up feedback also provided by the European Commission on April 2024 and the updates in the latest text of the CRA 2024/2847 (23 October 2024).

Table of Contents

1. Terms & Definitions, abbreviations

Abbreviations

For the purposes of the present document, the following abbreviations apply:

- BSI Bundesamt für Sicherheit in der Informationstechnik
- ANSSI Agence Nationale de la Sécurité des Systèmes d'Information
- CAB Conformity Assessment Body
- CC Common Criteria
- CCRA Common Criteria Recognition Agreement
- CEN European Committee for Standardization
- CENELEC European Committee for Electrotechnical Standardisation
- cPP Collaborative Protection Profile
- CRA Cyber Resilience Act (*see reference [CRA][1] in section 3 References*)
- CRA ESR Essential requirements from the Cyber Resilience Act
- DSO Distribution System Operator
- ECCG European Cybersecurity Certification Group
- ESMIG European association of smart energy solution providers
- ESR Essential Security Requirement
- ETR Evaluation Technical Report
- ETSI European Telecommunications Standards Institute
- EUCC European Union Cybersecurity Certification
- EUCC SPD Security Problem Definition in EUCC
- FW Firmware
- HW Hardware
- IDS Intrusion Detection System
- IEC International Electrotechnical Commission
- IPS Intrusion Prevention System
- ISO International Organization for Standardization
- ITSEF Information Technology Security Evaluation Facility
- NCCA National Cybersecurity Certification Authority
- PKI Public Key Infrastructure
- PP Protection Profile
- RTL Register Transfer Level
- SFR Security Functional Requirement
- SaaS Software as a Service
- SAR Security Assurance Requirement
- SBOM Software Bill of Materials
- SCCG Stakeholder Cybersecurity Certification Group
- SDO Standards Development Organization.
- SFP Security Function Policy
- SMGW Smart Meter Gateway

[1] Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act) (Text with EEA relevance)

- SPD Security Problem Definition
- ST Security Target
- SW Software
- TLS Transport Layer Security
- TOE Target Of Evaluation
- TSF TOE Security Functionality
- TSFI TSF Interface
- WAN Wide Area Network

Definitions

(1) ‘**product with digital elements’** means a software or hardware product and its remote data processing solutions, including software or hardware components being placed on the market separately;

(2) ‘**remote data processing’** means data processing at a distance for which the software is designed and developed by the manufacturer, or under the responsibility of the manufacturer, and the absence of which would prevent the product with digital elements from performing one of its functions;

(3) **‘software bill of materials**’ means a formal record containing details and supply chain relationships of components included in the software elements of a product with digital elements;

2. Introduction

2.1. Disclaimer

The study solely represents the views of ENISA and is without prejudice to the position of the European Commission and any of its initiatives, related or not to the CRA.

This study represents the views and analysis solely of ENISA, developed as part of a technical assessment conducted by subject matter experts. It aims to provide an in-depth examination of the interplay between the EU Cybersecurity Certification Framework (EUCC) and the Cyber Resilience Act (CRA), focusing on the technical and procedural aspects required to establish coherence between these two frameworks.

The analysis presented takes into account the legal and regulatory provisions of both the CRA and the EUCC framework, with conclusions and recommendations provided from a technical perspective. These should not be interpreted as legal advice, policy positions, or as representing the views of the European Commission.

This study is published without prejudice to the European Commission's position, whether related to the CRA or any other legislative or regulatory initiative. The content and conclusions herein are intended to contribute to the broader technical discourse and do not pre-empt or influence the formal stance of the European Commission or its institutions.

2.2. Preamble

The European Union has reinforced its approach to cybersecurity regulation with the Cyber Resilience Act (CRA), a comprehensive legislative framework that introduces horizontal cybersecurity requirements for all products with digital elements placed on the EU market. The CRA entered into force on 10 December 2024. It aims to address growing cybersecurity risks across sectors by laying out a set of essential requirements to ensure products are designed, developed, and maintained with security as a priority, thus enhancing the resilience of the EU's digital landscape. The CRA applies to all products with digital elements and categorizes them by risk level, including "important" and "critical" products that are subject to stricter cybersecurity obligations.

To provide manufacturers with flexible means of compliance, the CRA offers multiple pathways to demonstrate adherence to its essential requirements. These include European cybersecurity certification schemes, such as the EU Common Criteria (EUCC), as well as harmonized standards and recognized conformity assessment procedures. The CRA establishes a "presumption of conformity" for products that have been certified under a recognized European cybersecurity certification scheme, such as the EUCC, provided the certification meets at least a "substantial" assurance level, as specified in **Article 27**[2] of the CRA. However, obtaining an EUCC certification is not mandatory in order to obtain CRA compliance, even for products classified as important or critical. It is simply one pathway available to manufacturers who wish to leverage the EUCC's structured conformity processes as a means of meeting the CRA requirements.

[2] Article 27 CRA: "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 cybersecurity 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."

An essential aspect of the CRA framework its risk-based approach, with a clear focus on risk assessment considering not only the product category but also the specific use and security implications of each product. For example, smart cards used in different environments, such as a gym access card versus a card providing entry to a critical facility, carry inherently different levels of risk. While both products might fall under the same CRA product category, the potential impact on security is much greater for a smart card used in a sensitive, high-stakes environment. As such, the CRA requires manufacturers to determine appropriate assurance levels based on the risk profile and use context of the product, ensuring that cybersecurity measures are proportional to the security risks presented by each use case. Regarding the type of conformity assessment, the CRA allows the manufacturer to determine the appropriate procedure based on the risk profiles and use context, with stricter rules applying to some of the conformity assessment methods required for important and critical products.

Similarly to other EU product legislation within the New Legislative Framework (NLF), the CRA further expands compliance options through harmonized standards that specify technical criteria aligned with its essential cybersecurity requirements. To support this initiative, the European Commission intends to task the European Standardisation Organisations (CEN, Cenelec and ETSI) with developing 41 harmonized standards that cover both the horizontal cybersecurity requirements as well as product-specific standards for the important and critical categories of products with digital elements. This extensive standardization work aims to ensure that manufacturers across the EU have access to harmonized, state-of-the-art guidance, facilitating CRA compliance while fostering interoperability and consistency across the EU's digital market.

This report looks into the potential role of EUCC certification for CRA compliance, analysing how products may leverage EUCC certification to achieve presumption of conformity with the CRA requirements. While this report primarily examines the EUCC as an example of an EU certification scheme aligned with CRA requirements, it does not endorse EUCC certification as the preferred compliance method for important or critical products. Rather, it positions the EUCC as one option among the CRA's range of compliance tools, offering flexibility for manufacturers based on their specific cybersecurity needs and product profiles.

In carrying out this analysis, the report proposes an approach for assessing the EUCC in view of specifying its presumption of conformity in line with **Article 27** of the CRA. This preliminary assessment aims to support the EU's commitment to a flexible, adaptable regulatory landscape that meets high cybersecurity standards while supporting industry needs within a unified European market.

This study seeks to examine the technical aspects of implementing the CRA through the EUCC as a European cybersecurity certification scheme, focusing on its technical elements and provides potential conclusions that could be considered by the European Commission when establishing presumption of conformity. However, this study should not be read as providing guidelines for establishing presumption of conformity with the CRA, as the establishment of such presumption would require a formal legal act under the CRA in line with article 27(9).

2.3. Background

ENISA received late July 2023 from the European Commission a request of technical support for the preparation of the implementation of the CRA.

To develop, based on a comparative analysis between the CRA and the EUCC, **a proposal** for a way forward, including where needed **technical elements**, that would allow **the certification under EUCC to cover the essential cybersecurity requirements** and **conformity assessment obligations of the CRA**, and therefore to use EUCC certification to demonstrate conformity with the CRA in a seamless way.

This report has been prepared by ENISA and jtsec as contractor, aiming to fulfil the request mentioned above. A first draft was released by ENISA in November 2023, which received feedback from stakeholders and well as initial feedback from the European Commission services. The current document represents a second draft aiming to address such feedback, while also including some updates in order to take into account the changes in the legal text published on 20 November 2024[3], as well as the publication of the EUCC Implementing Act of 31 January 2024[4]. The current version of the report reflects and incorporates the feedback received from the ECCG and SCCG during the third quarter of 2024, following the internal distribution of an intermediate draft to these groups for review and input. The report offers an overview of relevant technical concepts from the CC and EUCC, and then offers a preliminary comparison between those concepts and the CRA. After identifying a set of SFRs and SARs that might be useful to implement this task, it then moves on to map the important and critical products as listed in Annex III and IV of the CRA on the CC/EUCC certification landscape, as any existing PPs covering those product categories should be considered with priority for the purposes of CRA implementation. Finally, the report discusses a number of strategies for implementation of CRA compliance through EUCC, notably by discussing the reuse of existing PPs and possibilities for closing existing gaps identified, concluding with a tentative timeline to guide such efforts.

It is important to note that this analysis is only exploratory at this stage and it shall not pre-empt any forthcoming decisions of the European Commission acting within its legal mandate under the CRA. This report represents a best-effort analysis by its authors and only represents their views. The report and its conclusions aim to serve as a basis for further discussion and to support the update of relevant PPs aiming to achieve CRA compliance.

At the time of this study, the Cyber Resilience Act has just been published and will have entered into force on the 10th of December of 2024. Following its entry into force, the CRA will be fully applicable after a 36-month transition period. The EUCC has been adopted on 31 January 2024 and will be applicable as of 27 February 2025. As manufacturers will start certifying under the EUCC, it is important to take into account the requirements of the CRA early on.

The possibility to provide presumption of conformity, including for European cybersecurity certification schemes adopted pursuant to Regulation (EU) 2019/881 (Cybersecurity Act), is set out in the CRA through Article 27 and related recitals 80 to 88. The CRA allows products with digital elements to be considered compliant with essential requirements if they adhere to harmonised standards, common specifications, or are certified under European cybersecurity certification schemes (see paragraphs 8 and 9). Specifically, products that meet harmonised standards published in the Official

[3] Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act), OJ L, 2024/2847, ELI: http://data.europa.eu/eli/reg/2024/2847/oj

[4] https://eur-lex.europa.eu/eli/reg_impl/2024/482/oj

Journal of the European Union or conform to common specifications established through EU implementing acts, are presumed to satisfy the CRA's essential requirements. Similarly, products certified under European cybersecurity certification schemes in accordance with Regulation (EU) 2019/881 are presumed compliant, provided the certification covers the relevant requirements and is at least at the 'substantial' assurance level.

Specifically, CRA Article 27 (8) establishes that *"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 cybersecurity 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."* . In line with Article 27 (9) and related recitals 82 and 83, the Commission is empowered to specify the presumption of conformity via a European cybersecurity certification scheme via a delegated act.

3. References

[CRA] REGULATION (EU) 2024/2847 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) No 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act) (https://eur-lex.europa.eu/eli/reg/2024/2847/oj)

[CSA] REGULATION (EU) 2019/881 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act).

[CCRA] Arrangement on the Recognition of Common Criteria Certificates In the field of Information Technology Security, July 2, 2014 (https://commoncriteriaportal.org/files/CCRA%20-%20July%202,%202014%20-%20Ratified%20September%208%202014.pdf)

[EUCC] COMMISSION IMPLEMENTING REGULATION (EU) 2024/482 of 31 January 2024 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)

[CEM2022] Common Methodology for Information Technology Security Evaluation. Evaluation methodology. November 2022. CEM:2022 Revision 1. CCMB-2022-11-001. (https://commoncriteriaportal.org/files/ccfiles/CEM2022R1.pdf)

[CC2022P1] Common Methodology for Information Technology Security Part 1: Introduction and general model. November 2022. CEM:2022 Revision 1. CCMB-2022-11-002 (https://commoncriteriaportal.org/files/ccfiles/CC2022PART1R1.pdf)

[CC2022P2] Common Methodology for Information Technology Security Part 2: Security functional components. November 2022. CEM:2022 Revision 1. CCMB-2022-11-002. (https://commoncriteriaportal.org/files/ccfiles/CC2022PART2R1.pdf)

[CC2022P3] Common Methodology for Information Technology Security Evaluation. Part 3: Security assurance components. November 2022. CEM:2022 Revision 1. CCMB-2022-11-003. (https://commoncriteriaportal.org/files/ccfiles/CC2022PART3R1.pdf)

[CC2022P4] Common Criteria for Information Technology Security Evaluation. Part 4: Framework for the specification of evaluation methods and activities. November 2022. CC:2022 Revision 1. CCMB-2022-11-004 (https://commoncriteriaportal.org/files/ccfiles/CC2022PART4R1.pdf)

[CC2022P5] Common Methodology for Information Technology Security. Part 5: Pre-defined packages of security requirements. November 2022. CEM:2022 Revision 1. CCMB-2022-11-005. (https://commoncriteriaportal.org/files/ccfiles/CC2022PART5R1.pdf)

[TR-03183] Technische Richtlinie TR-03183: Cyber-Resilienz-Anforderungen an Hersteller und Produkte. Teil 2: Software Bill of Materials (SBOM). Version 1.0. 2023-07-12.

[PP_APPSW] U.S. Government Approved Protection Profile - Protection Profile for Application Software Version 1.4

[PPFP_TLS] U.S. Government Approved Protection Profile - Functional Package for TLS Version 1.1

[CPP_FW] U.S. Government Approved Protection Profile - collaborative Protection Profile for Network Devices Version 3.0e

[PPMOD_IPS] U.S. Government Approved Protection Profile - PP-Module for Intrusion Prevention Systems (IPS), Version 1.0

[CPP_HARDCOPY] U.S. Government Approved Protection Profile - collaborative Protection Profile for Hardcopy Devices Version 1.0E

[PP_OS] U.S. Government Approved Protection Profile - Protection Profile for General Purpose Operating Systems Version 4.3

[NE8000_ST] Huawei NetEngine 8000 &NE9000 Series Routers' Software Security Target v1.0 (https://commoncriteriaportal.org/nfs/ccpfiles/files/epfiles/NSCIB-CC-0207368-STv1.2.pdf)

[CELLCRYPT_ST] Cellcrypt Android Mobile Client version 4.40 Security Target V1.2.3 (https://commoncriteriaportal.org/nfs/ccpfiles/files/epfiles/st_vid111278-st.pdf)

[PP_POI] Point of Interaction "POI-CHIP-ONLY" v2.0 (ANSSI-CC-PP-2010/08 to ANSSI-CC-PP-2010/10)

[PP_TACH_VU] BSI-CC-PP-0094-2017 for Digital Tachograph - Vehicle Unit (VU PP), Version 1.0

[PP_TACH_EFG] BSI-CC-PP-0092-2017 for Digital Tachograph - External GNSS Facility (EGF PP), Version 1.0
[PP_TACH_MS] BSI-CC-PP-0093-2017 for Digital Tachograph - Motion Sensor (MS PP), Version 1.0

[PP_CMCSOB] Cryptographic Module for CSP Signing Operations with Backup - PP CMCSOB, Version 0.35

[PP_CMKCKG] Cryptographic Module for CSP key generation services - PP CMCKG, version 0.35

[PP_CMCSO] Cryptographic Module for CSP Signing Operations without Backup - PP CMCSO, version 0.35

[PP_SMARTMETER_SMR] Protection Profile for Smart Meter Minimum Security requirements, Version: 1.0, Date: 30. October 2019, Authors: Ad-Hoc Group Privacy & Security of the CEN/CENELEC/ETSI Coordination Group on Smart Meters (https://www.commoncriteriaportal.org/nfs/ccpfiles/files/ppfiles/Protection%20Profile%20for%20Smart%20Meter%20Minimum%20Security%20requirements_v1-0.pdf).

[PP_SMARTMETER_SM] Protection Profile for the Security Module of a Smart Meter Gateway (Security Module PP), Version 1.0.3

[ISO_TS_9569] Evaluation criteria for IT security — Patch Management Extension for the ISO/IEC 15408 series and ISO/IEC 18045"

[SOGIS_SC_EVALUATION] Joint Interpretation Library Guidance for smartcard evaluation, Version 3.0, April 2024 (https://www.sogis.eu/documents/cc/domains/sc/JIL-Guidance-for-smartcard-evaluation-v3-0.pdf)

[PP_MRTD_PACE] PP for a Machine Readable Travel Document using Standard Inspection Procedure with PACE, v1.0.1 (https://www.sogis.eu/documents/cc/pp/sc/passport/pp0068_V2_ma1b.pdf)

[PP_MRTD_EAC] PP for a Machine Readable Travel Document with "ICAO Application" Extended Access Control, v1.10 (https://www.sogis.eu/documents/cc/pp/sc/passport/pp0056b.pdf)

[PP_MRTD_EAC_PACE] PP for a Machine Readable Travel Document with "ICAO Application" Extended Access Control with PACE, v1.3.2 (https://www.sogis.eu/uk/pp_pages/passport/pp_icao_eac_sac.html)

[PP_MRTD_BAC] PP for a Machine Readable Travel Document with "ICAO Application" Basic Access Control, V1.10 (https://www.sogis.eu/documents/cc/pp/sc/passport/pp0055b.pdf)

[PP_SSCD_KG] PP for a Secure Signature Creation Device - Part 2: Device with Key Generation, EN 419211-2:2013, V2.0.1 (https://commoncriteriaportal.org/nfs/ccpfiles/files/ppfiles/pp0059b_pdf.PDF)

[PP_SSCD_KI] PP for a Secure Signature Creation Device - Part 3: Device with key import, EN 419211-3:2013, V1.0.2 (https://commoncriteriaportal.org/nfs/ccpfiles/files/ppfiles/pp0075b_pdf.pdf)

[PP_SSCD_KGCG] PP for a Secure Signature Creation Device - Part 4: Extension for device with key generation and trusted communication with certificate generation application, EN 419211-4:2013, V1.0.1 (https://commoncriteriaportal.org/nfs/ccpfiles/files/ppfiles/pp0071b_pdf.pdf)

[PP_SSCD_KGSG] PP for a Secure Signature Creation Device - Part 5: Extension for device with key generation and trusted communication with signature creation application (https://commoncriteriaportal.org/nfs/ccpfiles/files/ppfiles/pp0072b_pdf.pdf)

[PP_SSCD_KISG] PP for a Secure Signature Creation Device - Part 6: Extension for device with key import and trusted communication with signature creation application (https://commoncriteriaportal.org/nfs/ccpfiles/files/ppfiles/pp0076b_pdf.pdf)

[PP_TACH_CARD] Digital Tachograph - Tachograph Card (TC), V1.0 (https://www.sogis.eu/documents/cc/pp/sc/tachograph_card/pp0091b.pdf)

[PP_IC] Security IC Platform PP with Augmentation Packages, v1.0, (https://www.sogis.eu/documents/cc/pp/sc/others/pp0084b.pdf)

[PP_JCOS_OPEN] Java Card System - Open Configuration, version 3.0.5 (December 2015) (https://www.sogis.eu/documents/cc/pp/sc/others/pp0099b.pdf)

[PP_JCOS_CLOSED] Java Card System - Closed Configuration, v3.0.5 (July 2018) (https://www.sogis.eu/documents/cc/pp/sc/others/pp0101b.pdf)

[PP_TPM] PP for a PC Client Specific Trusted Platform Module Family 2.0 Level 0 Revision 1.16, (https://www.sogis.eu/documents/cc/pp/sc/others/TCG_PP_PC_client_specific_TPM_SecV2_v10.pdf)

[PP_SIM] PP Universal SIM card, v2.0.2 (https://www.sogis.eu/documents/cc/pp/sc/others/ANSSI-CC-cible_PP-2010-04en.pdf)

[PP_eUICC] Embedded UICC for Machine-to-Machine Protection Profile, v1.1 (https://www.sogis.eu/documents/cc/pp/sc/others/pp0089b.pdf).

[PP_eUICC_CD] Embedded UICC for Consumer Devices, Protection Profile, Version 1.0 05-June-2018 (https://www.commoncriteriaportal.org/nfs/ccpfiles/files/ppfiles/pp0100b_pdf.pdf).

[GSMA_UICC] GSMA SGP.02 - Remote Provisioning Architecture for Embedded UICC Technical Specification, Versions 2.0, October 2014 and Version 3.0, 30 June 2015.

[PP_3S] BSI-CC-PP-0117-V2-2023 Secure Sub-System in System-on-Chip (3S in SoC), Version 1.8 (https://www.bsi.bund.de/SharedDocs/Zertifikate_CC/PP/aktuell/PP_0117.html).

[PP_ETSI_CMD] ETSI TS 103 732-1 V2.1.2 (2023-11), CYBER; Consumer Mobile Device; Part 1: Base Protection Profile (https://www.etsi.org/deliver/etsi_ts/103700_103799/10373201/02.01.02_60/ts_10373201v020102p.pdf).

[PP_ETSI_GSQKD] ETSI GS QKD 016 V2.1.1 (2024-01) Quantum Key Distribution (QKD); Common Criteria Protection Profile - Pair of Prepare and Measure Quantum Key Distribution Modules (https://www.etsi.org/deliver/etsi_gs/QKD/001_099/016/02.01.01_60/gs_QKD016v020101p.pdf).

[CIU9872B_ST] Security target Lite of HED Secure Chip CIU9872B_01 C13 with IC Dedicated Software Version 1.1, Date 2020-03-25 (https://www.tuv-nederland.nl/assets/files/cerfiticaten/2020/04/security-target-lite-of-ciu9872b_01-c13-secure-chip_v1_1.pdf)

[CC_TRANSITION] Transition Policy to CC:2022 and CEM:2022**,** Document Number: CCMC-2023-04-001 Date: April 20th, 2023 (https://commoncriteriaportal.org/files/ccfiles/CC2022CEM2022TransitionPolicy.pdf)

[SOG-IS MRA] Mutual Recognition Agreement of Information Technology Security Certificates, Version 3.0, 08 Jan. 2010 (https://www.sogis.eu/documents/mra/20100107-sogis-v3.pdf).

[ISO_51] ISO/IEC Guide 51:2014 Safety aspects — Guidelines for their inclusion in standards, Edition 3, 2014.

[ISO_14971_2019] ISO 14971:2019. Medical devices — Application of risk management to medical devices. Edition 3, 2019.

[SOGIS_CRYPTO] SOG-IS Crypto Evaluation Scheme Agreed Cryptographic Mechanisms, Version 1.3 February 2023 (https://www.sogis.eu/documents/cc/crypto/SOGIS-Agreed-Cryptographic-Mechanisms-1.3.pdf).

4. Relevant EUCC concepts for this study

The European Common Criteria-based cybersecurity certification scheme (EUCC) Implementing Regulation 2024/482 [EUCC] is designed to facilitate the cybersecurity certification of ICT products within the European Union, ensuring compliance with ISO/IEC 15408 and the Common Criteria (CC). Under the EUCC scheme, ICT products must undergo a cybersecurity evaluation process following the rules and evaluation methodology of the Common Criteria standard.

This report has been published within the timeframe between the entry into force of the EUCC and the 12 months of transition period before its application. Therefore, at the time this document was written, no EUCC certificates had been issued yet, and no EUCC-certified products existed on the market. For illustrative purposes, the following explains the process by which ICT products that undergo cybersecurity evaluations can obtain Common Criteria certifications under a national Common Criteria scheme. In the future, the EUCC will replace existing national schemes in the European Union.

Manufacturers of ICT products that implement cybersecurity-related functionality and wish to obtain a CC certificate, have apply at a certification body and engage in Common Criteria evaluations conducted by an Information Technology Security Evaluation Facility (ITSEF). In these evaluations, the ITSEF conducts cybersecurity assessments under the Common Criteria evaluation methodology, which includes reviewing the product's technical documentation, functional testing of security features, vulnerability analysis, and penetration testing. The Certification Body is responsible for issuing a Common Criteria certificate for the evaluated product upon the successful outcome of the evaluation. According to the CCRA/SOGIS, the certification Body has to be accredited and it could be either a public entity, or a privately owned one that is oversighted by the governmental body for permission to issue a certificate with the CCRA and/or SOGIS logo.

Common Criteria certificates issued by one country (i.e., a national Certification Body) are recognized by other countries in accordance to two existing international mutual recognition mechanisms: The Common Criteria Recognition Arrangement [CCRA] gathers 31 countries[5], including 14 Member States and the SOG-IS Mutual Recognition Agreement [SOG-IS MRA] gathers 15 Member States as well as Norway and the UK[6]. Both aim for mutual recognition of the evaluation and certification of IT security products under the CC framework, though they operate at different levels of ambitions. The CCRA is an international arrangement that allows for the mutual recognition of security evaluations across countries globally up to EAL2. In contrast, the SOG-IS MRA is a European-focused agreement that ensures mutual recognition of IT security certificates among European countries up to EAL4. Countries under these arrangements are classified into issuing countries, those entitled to issue CC certificates, and consumer countries, those that recognize certificates from issuing countries but that don't issue certificates themselves.

At the date of release of this report, EUCC will change the paradigm of certificate recognition among countries in the European Union by introducing a number of changes in the obligations and governance structure of common criteria certification, and by extending mutual recognition across the whole EU. In this context, the EUCC will have an impact on the existing mutual recognition

[5] https://www.commoncriteriaportal.org/ccra/members/index.cfm

[6] https://www.sogis.eu/

arrangements SOG-IS and CCRA. Therefore, this document should be seen as a live report that will require further updates.

Cybersecurity evaluation and certification processes carried out under the EUCC scheme will be articulated around various key concepts of the Common Criteria. Those that condition and influence the evaluation to the greatest extent are three: **The Target of Evaluation (TOE), the Security Functional Requirements (SFRs) and Security Assurance Requirements (SARs)**. This section aims to provide an entry-level introduction of the aforementioned elements that is sufficient for the reader to understand how such mechanisms interplay with CRA in further sections of the study. Another concept in the EUCC/CC that has considerable relevance in this study, remarkably two: the **Security Problem Definition**, that is further elaborated in section **4.4 Other relevant elements in EUCC/CC**, along with other important concepts. All of these elements are defined in the **Security Target**, which is the key document in CC.

In the context of the objective of the current study, this document hereafter refers to SFRs and SARs together as **"EUCC technical elements".** Given that EUCC certifications have been issued at the date of release of this documents, however ongoing and future EUCC evaluations will be fully based on CC methodology, therefore this report refers sometimes to certain aspects of the methodology pointing to CC instead of to EUCC, whereas EUCC term is used to reference to the scheme or its related processes. It will however point to relevant aspects that are specific to the EUCC scheme. The Common Criteria (CC) and Common Criteria Evaluation methodology (CEM) is the cybersecurity assessment framework utilized within the EUCC framework, making it the source of these technical elements.

4.1. Target of Evaluation (TOE)

The **Target of Evaluation (TOE)** is a core concept of established by the CC standard, [CC2022P1] (https://commoncriteriaportal.org/files/ccfiles/CC2022PART1R1.pdf) that defines the boundary of the evaluation. There are cases where the TOE matches with the ICT product, but it might not be always the case and the TOE may consist of a part of an IT product, or a set of IT products (i.e. in distributed systems). In practice, it is a quite common scenario that the TOE consists of only a part of the product or a subset of it and, as such, the TOE and the product have different boundaries.

In CC evaluations, the assessment of the applicable cybersecurity requirements will scope only the TOE, so it is possible that some parts of the product aren't covered by the evaluation and the certification. Every other element other than the TOE that is required by the TOE to function or operate as expected is denominated ***operational environment*** and it is not covered by the evaluation. It might consist of elements such as hardware platforms, operating systems, IT elements in the network or, where the scope of the product doesn't match the scope of the TOE, parts of the product outside the TOE boundary.

The TOE may consist of hardware, software, firmware or a combination of them. The main point of impact associated to the concept of the TOE, as previously outlined, is the fact that the parts of the ICT product not included in the scope of the TOE aren't included in the evaluation and therefore under EUCC they don't need to meet the cybersecurity requirements under evaluation. Choosing a specific TOE scope is a decision that always must consider that the TOE scope shall comprise, as a minimum, those the parts of the product that implement the Security Functional Requirements. CC evaluations have been, thorough and complex and, as such, the overall complexity, required time and cost are usually dependent on the size of the TOE scope. Moreover, in certain scenarios the security assurance provided by the evaluation can be guaranteed only in certain parts of the product that are those implementing the security modules and other parts of the product or subcomponents of a complex system might not have strict security requirements. At the date of publication of this report, the current version of CC 2022 has introduced the concept of *multi-assurance*, which contemplates defining different security levels within the scope of TOEs, and therefore facilitating full-product scopes in certain cases of CC evaluations where the implementation of the security aspects is localized only in specific parts of the product. However, a multi-assurance evaluation can only be used in combination with a PP-configuration as defined in [CC2022P1]. Moreover, at the date of publication of this report, multi-assurance has not been put into practice in the industry in a mainstreamed manner. As such, in non-multi-assurance scenarios, choosing scopes larger could be either unfeasible or counterproductive in a EUCC/CC certification campaign.

Nonetheless, the chosen TOE scope shall be always appropriate and adequate with respect to the evaluated security functionality and with the intended purpose of the product. Depending on each evaluation, the scope of the TOE can be freely chosen by the manufacturer of the product or, if the evaluation uses conformance with a Protection Profile the TOE scope can be determined by that Protection Profile. Protection Profiles are documents that are used to harmonize the TOE and other relevant elements of a EUCC/CC certification for products that belong to similar technological or market categories (see section **4.4 Other relevant elements in EUCC/CC** for details on this concept).

4.2. Security Functional Requirements (SFRs)

The **Security Functional Requirements (SFRs)** consist of requirements regarding functionalities related to cybersecurity aspects that the product under evaluation must meet[7]. They describe in a generic manner *security mechanisms* and *security services* to be implemented by the product.

The author of this study identifies two categories of security functionalities that can be described by the SFRs and that can be broadly summarised as follows:

- Security mechanisms, that are meant to counter a threat to the assets protected by the TOE. For example, encrypting saved password to avoid their disclosure.
- Security services, which don't counter any threat but are meant to enforce organisational security policies. For example, providing a cryptographic signature service to users of the TOE.

The CC standard defines in [CC2022P2] a number of SFRs that are structured in functional classes, which are further divided into functional families. Classes and families group together SFRs for which the type of functionality described by the requirement has some common relationship, i.e., all SFRs related to cryptographic functionality belong to the same class and they are organized in families that encompass requirements related to different cryptographic aspects such as cryptographic key management or cryptographic operations. There are 11 functional classes in CC, that are listed below:

- Class FAU: Security Audit.
- Class FCO: Communication.
- Class FCS: Cryptographic support.
- Class FDP: User data protection.
- Class FIA: Identification and authentication.
- Class FMT: Security management.
- Class FPR: Privacy.
- Class FPT: Protection of the TSF.
- Class FRU: Resource utilisation.
- Class FTA: TOE access.
- Class FTP: Trusted path/channels.

[7] The formal definition of the SFR concept can be found in [CC2022P1].

SFRs are named according to a nomenclature that follows the structure ***FXX_YYY.N***, where F*XX* identifies the functional class, *YYY* identifies the functional family and *N* identifies the functional component (SFR) within that family.

The following diagram summarizes the existing functional families in [CC2022P2] and their main functional area.

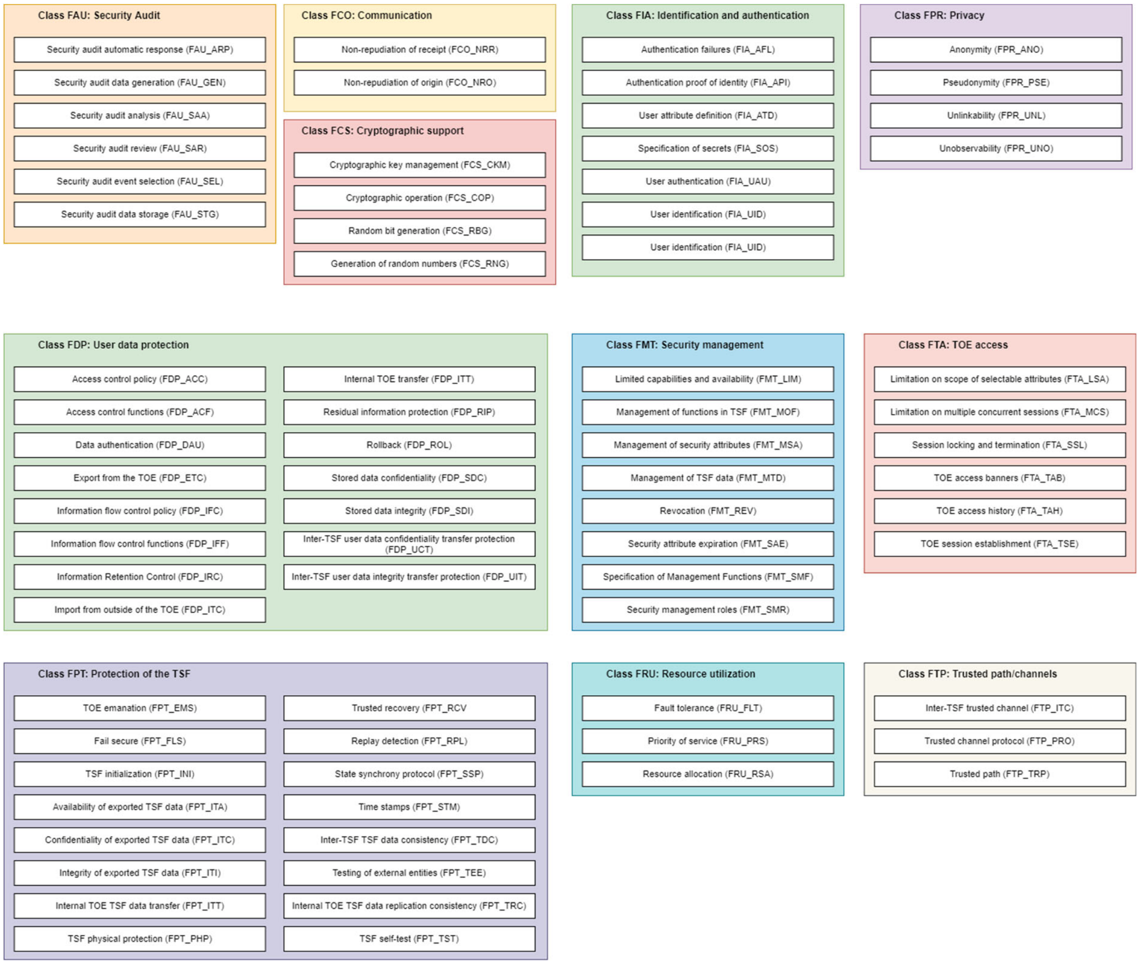

Class FAU: Security Audit
Security audit automatic response (FAU_ARP)
Security audit data generation (FAU_GEN)
Security audit analysis (FAU_SAA)
Security audit review (FAU_SAR)
Security audit event selection (FAU_SEL)
Security audit data storage (FAU_STG)
Class FCO: Communication
Non-repudiation of receipt (FCO_NRR)
Non-repudiation of origin (FCO_NRO)
Class FCS: Cryptographic support
Cryptographic key management (FCS_CKM)
Cryptographic operation (FCS_COP)
Random bit generation (FCS_RBG)
Generation of random numbers (FCS_RNG)
Class FIA: Identification and authentication
Authentication failures (FIA_AFL)
Authentication proof of identity (FIA_API)
User attribute definition (FIA_ATD)
Specification of secrets (FIA_SOS)
User authentication (FIA_UAU)
User identification (FIA_UID)
User identification (FIA_UID)
Class FPR: Privacy
Anonymity (FPR_ANO)
Pseudonymity (FPR_PSE)
Unlinkability (FPR_UNL)
Unobservability (FPR_UNO)
Class FDP: User data protection
Access control policy (FDP_ACC)
Access control functions (FDP_ACF)
Data authentication (FDP_DAU)
Export from the TOE (FDP_ETC)
Information flow control policy (FDP_IFC)
Information flow control functions (FDP_IFF)
Information Retention Control (FDP_IRC)
Import from outside of the TOE (FDP_ITC)
Internal TOE transfer (FDP_ITT)
Residual information protection (FDP_RIP)
Rollback (FDP_ROL)
Stored data confidentiality (FDP_SDC)
Stored data integrity (FDP_SDI)
Inter-TSF user data confidentiality transfer protection (FDP_UCT)
Inter-TSF user data integrity transfer protection (FDP_UIT)
Class FMT: Security management
Limited capabilities and availability (FMT_LIM)
Management of functions in TSF (FMT_MOF)
Management of security attributes (FMT_MSA)
Management of TSF data (FMT_MTD)
Revocation (FMT_REV)
Security attribute expiration (FMT_SAE)
Specification of Management Functions (FMT_SMF)
Security management roles (FMT_SMR)
Class FTA: TOE access
Limitation on scope of selectable attributes (FTA_LSA)
Limitation on multiple concurrent sessions (FTA_MCS)
Session locking and termination (FTA_SSL)
TOE access banners (FTA_TAB)
TOE access history (FTA_TAH)
TOE session establishment (FTA_TSE)
Class FPT: Protection of the TSF
TOE emanation (FPT_EMS)
Fail secure (FPT_FLS)
TSF initialization (FPT_INI)
Availability of exported TSF data (FPT_ITA)
Confidentiality of exported TSF data (FPT_ITC)
Integrity of exported TSF data (FPT_ITI)
Internal TOE TSF data transfer (FPT_ITT)
TSF physical protection (FPT_PHP)
Trusted recovery (FPT_RCV
Replay detection (FPT_RPL)
State synchrony protocol (FPT_SSP)
Time stamps (FPT_STM)
Inter-TSF TSF data consistency (FPT_TDC)
Testing of external entities (FPT_TEE)
Internal TOE TSF data replication consistency (FPT_TRC)
TSF self-test (FPT_TST)
Class FRU: Resource utilization
Fault tolerance (FRU_FLT)
Priority of service (FRU_PRS)
Resource allocation (FRU_RSA)
Class FTP: Trusted path/channels
Inter-TSF trusted channel (FTP_ITC)
Trusted channel protocol (FTP_PRO)
Trusted path (FTP_TRP)

Figure 1 Security Functional families in Common Criteria

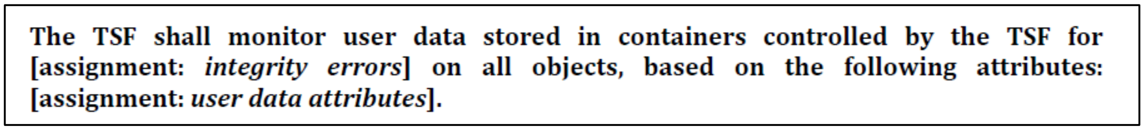
[CC2022P2] can be seen as a catalogue of SFRs available for manufacturers of ICT products to include in the scope of the evaluations. It is not intended that all the SFRs of [CC2022P2] are included in every evaluation, and not all products being certified under EUCC are meant to implement mechanisms that meet all the SFRs. Manufacturers choose those SFRs that are covered by the evaluation based on the type of product, the IT assets that the product needs to protect from certain attack scenarios, and the security mechanisms that their product implement in order to mitigate the threats applicable to those scenarios. As a way to harmonize application, Protection Profiles (see section **4.4 Other relevant elements in EUCC/CC**) define the SFRs to be included in an evaluation for a specific type of product contemplated by that Protection Profile.

The combined functionality of all components in the TOE scope that is relied upon for the correct enforcement of the SFRs is what is termed the **TOE Security Functionality (TSF)**, and it defines the logical boundary of the Target of Evaluation.

SFRs are formulated in a generic way, as they are intended to be valid and applicable in a high variety of heterogeneous types of ICT products. Therefore, they are written in a way that tends to be more abstract and omitting the inclusion of implementation details. In simpler terms, SFRs indicates what the TOE needs to do, but not how it needs to be done. For example, SFRs included in the FDP class (for User Data Protection), which are meant to protect user data managed by the TOE, indicate the requirements for protection of such data (e.g., the TOE shall protect the confidentiality of user data at rest), but don't mention what mechanisms (e.g., cryptography or access control) need to be implemented in order to provide such protection.

Some of the SFRs in [CC2022P2] are written in a way that allows customization of certain parts of the requirement at the moment of instantiation of the SFR. This is achieved by including in it open statements that shall be completed or filled by the manufacturer of the product under certification, making the final text of the requirement more specific for that particular product.

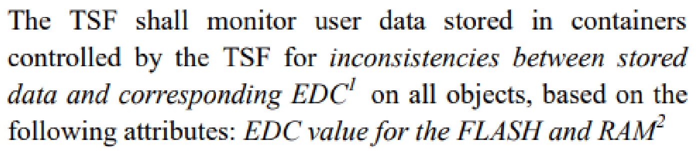
An example for the SFR *FDP_SDI.1 Stored data integrity monitoring*, taken from [CC2022P2] can be seen in the figure below.



The TSF shall monitor user data stored in containers controlled by the TSF for [assignment: *integrity errors*] on all objects, based on the following attributes: [assignment: *user data attributes*].

Figure 2 Example of SFR with open parts from [CC2022P2]

The parts of the requirement text in the figure that are between square brackets and contain the keyword *assignment* are meant to be replaced by specific details upon instantiation of the SFR. For example, the manufacturer is expected to indicate which kind of integrity errors are monitored and based on which user data attributes, e.g., detect unauthorized modification of data based on a CRC32 checksum. The image below shows an example of how the final text of the requirement would look like in a real case, taken from [CIU9872B_ST] (note: EDC in the picture stands for "Error Data Check").



The TSF shall monitor user data stored in containers controlled by the TSF for *inconsistencies between stored data and corresponding EDC*[1] on all objects, based on the following attributes: *EDC value for the FLASH and RAM*[2]

Figure 3 Example of instantiation of a SFR in [CIU9872B_ST]

SFRs are often organized within functional families in a hierarchical structure. This means that when an SFR at a higher level in the hierarchy is included in an evaluation and met, all SFRs positioned below it in the hierarchy are automatically considered met as well. This hierarchical relationship simplifies the evaluation process by ensuring that meeting a higher-level requirement guarantees the fulfilment of related lower-level requirements. An example can be seen in the image below:

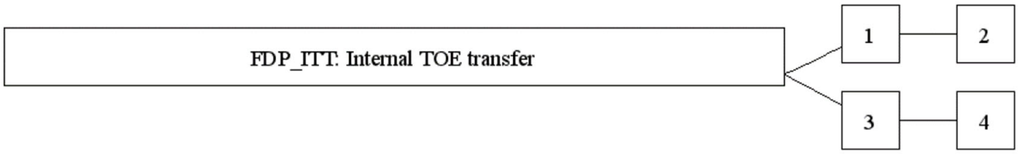
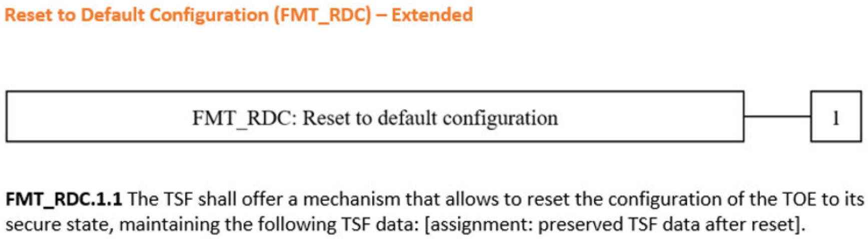


Figure 4 Example of hierarchical relationships within functional families ([CC2022P2])

The figure shows the four Security Functional Requirements existing in the functional family *FDP_ITT: Internal TOE transfer*, which are FDP_ITT.1, FDP_ITT.2, FDP_ITT.3 and FDP_ITT.4. The horizontal line linking FDP_ITT.1 and FDP_ITT.2 indicates that FDP_ITT.2 is hierarchically above FDP_ITT.1; the same situation occurs between FDP_ITT.3 and FDP_ITT.4. The text of FDP_ITT.2 contains all the elements that exist in the text of FDP_ITT.1, and additional ones, hence if FDP_ITT.2 is met then FDP_ITT.1 is met as well, and that same relationship exists between FDP_ITT.3 and FDP_ITT.4. However, the image also depicts that FDP_ITT.1-FDP_ITT.2 and FDP_ITT.3- FDP_ITT.4 are organized in different branches in the hierarchy, meaning that no hierarchical relationship exists between the elements located in each separate branch. For example, FPT_ITT.4 has no hierarchical relationship with FDP_ITT.1, therefore meeting FDP_ITT.4 doesn't mean that FDP_ITT.1 is met.

Despite the extensive range of security classes and families included in [CC2022P2], there may be instances where a product being evaluated has specific security features not covered by existing SFRs in the Common Criteria standard. In such cases, the Common Criteria framework allows for the creation of **Extended SFRs**. These are custom SFRs, different from those in [CC2022P2], and must be written according to the standardized language and conventions defined the Common Criteria standard, e.g., they need to be organised within functional classes and families. They describe the security functionalities implemented by the TOE that lack an equivalent SFR in [CC2022P2].

As an illustrative example, the Annex to this study defines the extended component named "FMT_RDC.1: Reset to default configuration", which defines security functionality for a mechanism that allows resetting to a default configuration. Such functionality is not covered by any of the SFRs currently existing in [CC2022P2], therefore it was necessary to define an extended SFR for such purpose:



Reset to Default Configuration (FMT_RDC) – Extended

FMT_RDC: Reset to default configuration
1

FMT_RDC.1.1 The TSF shall offer a mechanism that allows to reset the configuration of the TOE to its secure state, maintaining the following TSF data: [assignment: preserved TSF data after reset].

Figure 5 Definition of FMT_RDC: Reset to default configuration

The security features described by the SFRs in the scope of the evaluation shall be implemented **only** by those parts of the ICT product that fall within the scope of the Target of Evaluation (TOE). The operational environment can implement some security mechanisms that overall help in the protection of relevant assets, but those won't be included as part of the evaluation, even if they are implemented by the same product, since they are out of the TOE scope. During a EUCC evaluation, the TOE will be tested for correct implementation and enforcement of the security features described by the SFRs in scope of the evaluation.

An illustrative example can be seen in the picture below, where the full product consists in a network device (i.e., a firewall) and a remote management console for the device that is hosted in the cloud. The scope of the TOE would typically comprise only the device installed on-premises, but not the part of the solution that resides in the remote cloud. Section **5.4 Scope of the assessment in EUCC vs CRA** will further discuss on how the part of the solution that resides in the remote cloud could be considered in the light of the notion of "remote data processing" included in the CRA.

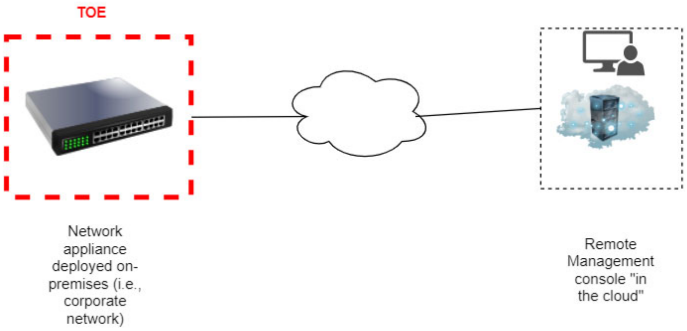

TOE
Network appliance deployed on-premises (i.e., corporate network)
Remote Management console "in the cloud"

Figure 6 Example of TOE scope being different from the full product scope

4.3. Security Assurance Requirements (SARs)

[CC2022P1] defines the Security Assurance Requirements as "a description of how the TOE is to be evaluated" or "a description of how assurance is to be gained that the TOE meets the SFRs". They are a specific type of security requirement that don't scope the security functionality of the TOE, but they define what will be assessed during the EUCC evaluation or, in other words, the different assessment activities that will take place during the evaluation.

SARs establish requirements for one or more of the following:

- **Manufacturers** (developers of products under evaluation), e.g., to deliver the TOE to the ITSEF, to elaborate user guidance, to provide design information for the evaluation, etc.
- **Evidence used as input for the evaluation**, by establishing the content and presentation elements that such evidence need include, e.g. TOE guidance, design information, manufacturer's processes.
- **Evaluators,** as action elements defining each of the assessment activities that the ITSEFs shall carry out on the TOE and other evidence during the evaluation, i.e. to confirm that the user guidance meets the related content and presentation elements defined for it by the applicable SARs.

With regards to the requirements for evaluators included in the SARs, the [CEM2022] (https://commoncriteriaportal.org/files/ccfiles/CEM2022R1.pdf) defines the evaluation methodology that they shall follow in order to conduct the evaluation activities linked to the evaluator action items included in the SARs of [CC2022P3] (https://commoncriteriaportal.org/files/ccfiles/CC2022PART3R1.pdf) .

SARs follow the same structural format as the SFRs: they are structured within *assurance classes*, that are further divided into *assurance families*, which group together SARs that are related to the same verification aspects. SARs are named following the format ***AXX_YYY.N***, where AXX identifies the assurance class, YYY the assurance family within the class, and N the assurance component (SAR) within the family.

An example of the above can be depicted taking from [CC2022P3] the decomposition of the ADV_TDS assurance family (TOE Design) into its different Security Assurance Requirements:

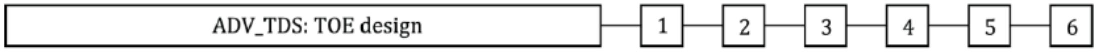


Figure 7 Decomposition of ADV_TDS assurance family

As shown in the figure, ADV_TDS family is comprised of the SARs ADV_TDS.1, ADV_TDS.2, ADV_TDS.3, ADV_TDS.4, ADV_TDS.5 and ADV_TDS.6.

[CC2022P3] includes assurance families and classes with SARs that cover diverse aspects relevant for evaluations, such as TOE design documentation, TOE guidance, TOE testing documentation, life-cycle aspects and manufacturer's procedures impacting the security of the TOE during its lifecycle (such as configuration management, security in development sites, or flaw remediation), TOE vulnerability assessment during the evaluation, among others (see section **4.1 Target of Evaluation (TOE)**).

The figure below summarizes the assurance classes and families included in the CC standard.

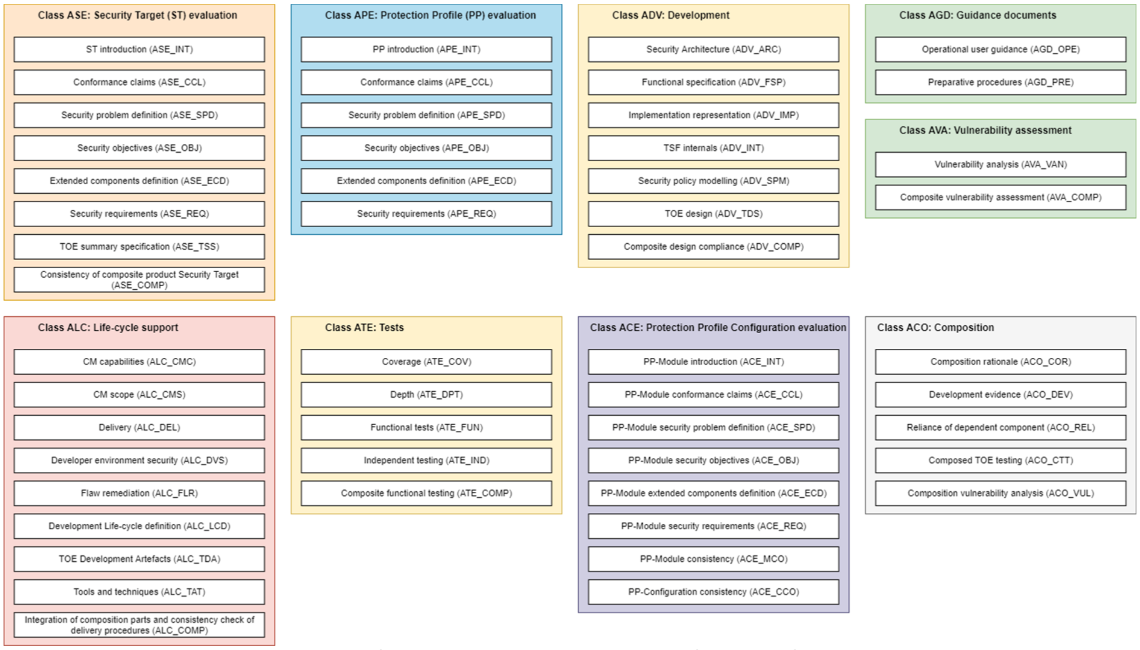

Class ASE: Security Target (ST) evaluation
ST introduction (ASE_INT)
Conformance claims (ASE_CCL)
Security problem definition (ASE_SPD)
Security objectives (ASE_OBJ)
Extended components definition (ASE_ECD)
Security requirements (ASE_REQ)
TOE summary specification (ASE_TSS)
Consistency of composite product Security Target (ASE_COMP)
Class APE: Protection Profile (PP) evaluation
PP introduction (APE_INT)
Conformance claims (APE_CCL)
Security problem definition (APE_SPD)
Security objectives (APE_OBJ)
Extended components definition (APE_ECD)
Security requirements (APE_REQ)
Class ADV: Development
Security Architecture (ADV_ARC)
Functional specification (ADV_FSP)
Implementation representation (ADV_IMP)
TSF internals (ADV_INT)
Security policy modelling (ADV_SPM)
TOE design (ADV_TDS)
Composite design compliance (ADV_COMP)
Class AGD: Guidance documents
Operational user guidance (AGD_OPE)
Preparative procedures (AGD_PRE)
Class AVA: Vulnerability assessment
Vulnerability analysis (AVA_VAN)
Composite vulnerability assessment (AVA_COMP)
Class ALC: Life-cycle support
CM capabilities (ALC_CMC)
CM scope (ALC_CMS)
Delivery (ALC_DEL)
Developer environment security (ALC_DVS)
Flaw remediation (ALC_FLR)
Development Life-cycle definition (ALC_LCD)
TOE Development Artefacts (ALC_TDA)
Tools and techniques (ALC_TAT)
Integration of composition parts and consistency check of delivery procedures (ALC_COMP)
Class ATE: Tests
Coverage (ATE_COV)
Depth (ATE_DPT)
Functional tests (ATE_FUN)
Independent testing (ATE_IND)
Composite functional testing (ATE_COMP)
Class ACE: Protection Profile Configuration evaluation
PP-Module introduction (ACE_INT)
PP-Module conformance claims (ACE_CCL)
PP-Module security problem definition (ACE_SPD)
PP-Module security objectives (ACE_OBJ)
PP-Module extended components definition (ACE_ECD)
PP-Module security requirements (ACE_REQ)
PP-Module consistency (ACE_MCO)
PP-Configuration consistency (ACE_CCO)
Class ACO: Composition
Composition rationale (ACO_COR)
Development evidence (ACO_DEV)
Reliance of dependent component (ACO_REL)
Composed TOE testing (ACO_CTT)
Composition vulnerability analysis (ACO_VUL)

Figure 8 Security Assurance Families in Common Criteria

The assessment activities that will be conducted during the evaluation will be those resulting from the combination of SARs chosen to be included during the evaluation. It is not mandatory to include all assurance classes, families or components in the evaluation. As in the case of the SFRs, SARs can be structured hierarchically within families and if a SAR included in the evaluation is met, then the SARs placed hierarchically below that one are automatically met as well. This situation can be illustrated with an example, as shown in the figure below:

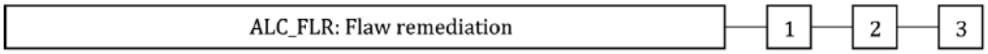
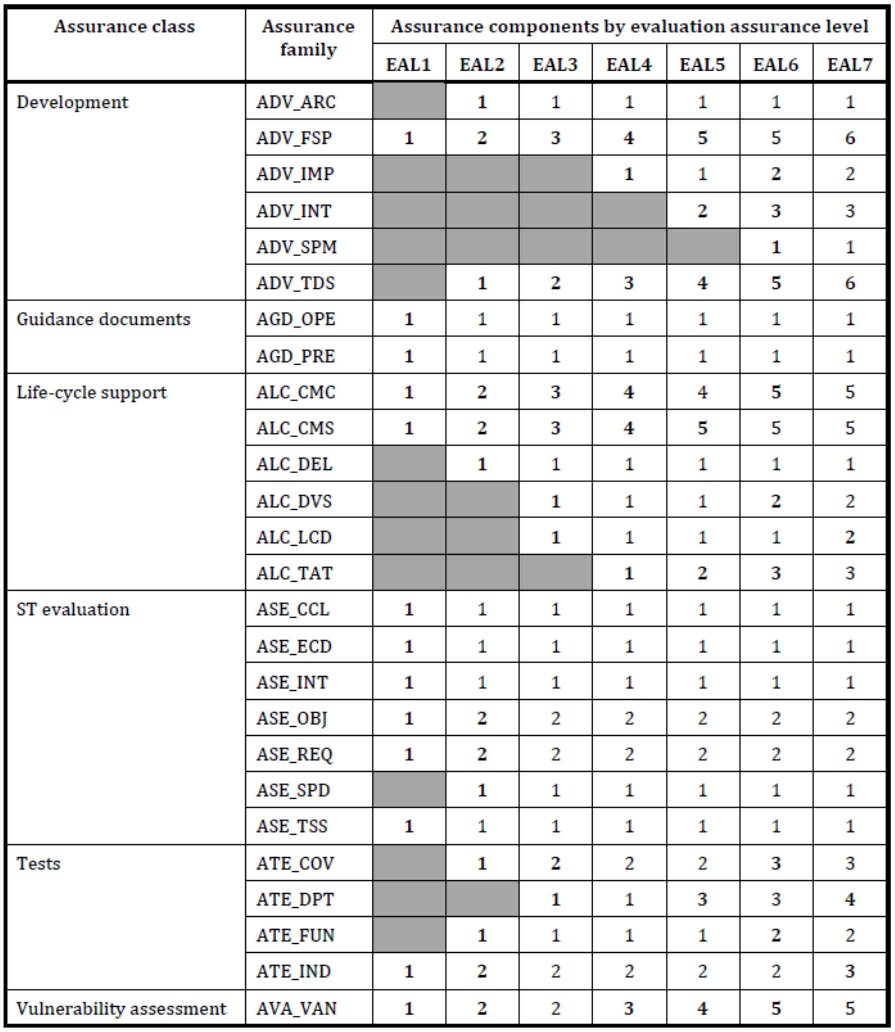


Figure 9 Decomposition of assurance family ALC_FLR Flaw remediation

As can be seen in the above picture, the ALC_FLR family is comprised of the SARs ALC_FLR.1, ALC_FLR.2 and ALC_FLR.3. ALC_FLR.2 is hierarchically above ALC_FLR.1 and ALC_FLR.3 is hierarchically above ALC_FLR.2 (and hence above ALC_FLR.1 as well).

The SARs are included in the evaluations typically through assurance packages, which are sets of SARs. Common Criteria provides a set of seven assurance packages that have been identified as useful in support of common usage. Each of them is named "**Evaluation Assurance Level (EAL)**", with EAL1 being the lowest and EAL7 the highest. Evaluation Assurance Levels also have a hierarchical relationship, given through the hierarchical relations between the SARs in each EAL. Therefore, each EAL is meant to offer the same degree of assurance as the one immediately below plus certain additional assurance. The contents of the assurance package (the SARs in it) don't depend on the type of product being evaluated, they are designed to be used as is in the evaluation of any type of product.

The figure below shows the decomposition of each EAL into the SARs contained in them, which is taken from [CC2022P5] (https://commoncriteriaportal.org/files/ccfiles/CC2022PART5R1.pdf):



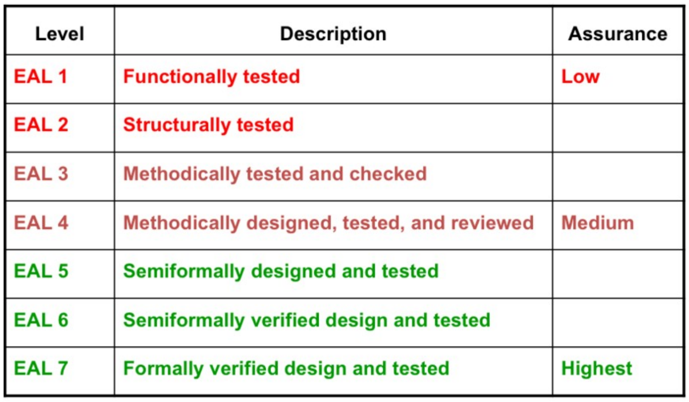
Assurance class	Assurance family	Assurance components by evaluation assurance level						
		EAL1	EAL2	EAL3	EAL4	EAL5	EAL6	EAL7
Development	ADV_ARC		1	1	1	1	1	1
	ADV_FSP	1	2	3	4	5	5	6
	ADV_IMP				1	1	2	2
	ADV_INT					2	3	3
	ADV_SPM						1	1
	ADV_TDS		1	2	3	4	5	6
Guidance documents	AGD_OPE	1	1	1	1	1	1	1
	AGD_PRE	1	1	1	1	1	1	1
Life-cycle support	ALC_CMC	1	2	3	4	4	5	5
	ALC_CMS	1	2	3	4	5	5	5
	ALC_DEL		1	1	1	1	1	1
	ALC_DVS			1	1	1	2	2
	ALC_LCD			1	1	1	1	2
	ALC_TAT				1	2	3	3
ST evaluation	ASE_CCL	1	1	1	1	1	1	1
	ASE_ECD	1	1	1	1	1	1	1
	ASE_INT	1	1	1	1	1	1	1
	ASE_OBJ	1	2	2	2	2	2	2
	ASE_REQ	1	2	2	2	2	2	2
	ASE_SPD		1	1	1	1	1	1
	ASE_TSS	1	1	1	1	1	1	1
Tests	ATE_COV		1	2	2	2	3	3
	ATE_DPT			1	1	3	3	4
	ATE_FUN		1	1	1	1	2	2
	ATE_IND	1	2	2	2	2	2	3
Vulnerability assessment	AVA_VAN	1	2	2	3	4	5	5

Figure 10 Decomposition of EALs in [CC2022P5]

The figure above shows, for instance, that EAL2 is composed of the following SARs:

- ADV_ARC.1 Security architecture description
- ADV_FSP.2 Security-enforcing functional specification
- ADV_TDS.1 Basic design
- AGD_OPE.1 Operational user guidance
- AGD_PRE.1 Preparative Procedures
- ALC_CMC.2 Use of the CM system
- ALC_CMS.2 Parts of the TOE CM coverage
- ALC_DEL.1 Delivery procedures
- ASE_CCL.1 Conformance claims
- ASE_ECD.1 Extended components definition
- ASE_INT.1 ST Introduction
- ASE_OBJ.2 Security objectives
- ASE_REQ.2 Derived security requirements
- ASE_SPD.1 Security problem definition
- ASE_TSS.1 TOE summary specification
- ATE_COV.1 Evidence of coverage
- ATE_FUN.1 Functional testing
- ATE_IND.2 Independent testing - sample
- AVA_VAN.2 Vulnerability analysis

EALs are designed in such a way that a given EAL is meant to provide an established degree of assurance through the combination of the SARs included in it. Thus, an EAL is a sound way to create an immediate relationship between a set of assurance activities and the value or criticality of the assets to be protected by the TOE subject of that evaluation. EAL1 and EAL2 are considered in the industry *low assurance* packages, whereas EAL3 and EAL4 are considered *medium assurance*, and EAL5-7 are considered *high assurance.* Each assurance package can be identified with a designated name within the CC standard.



Level	Description	Assurance
EAL 1	Functionally tested	Low
EAL 2	Structurally tested	
EAL 3	Methodically tested and checked	
EAL 4	Methodically designed, tested, and reviewed	Medium
EAL 5	Semiformally designed and tested	
EAL 6	Semiformally verified design and tested	
EAL 7	Formally verified design and tested	Highest

Figure 11 denomination and assurance level of EALs

For example, consumer software and devices are usually certified using low assurance, however devices used in payment industry are certified using EALs between 4 and 5, and IT products deployed in military or aerospace environments are typically certified to EAL6 or EAL7. The selection of an EAL must be appropriate with respect to the value of the assets to be protected. When using Protection Profiles (see section **4.4 Other relevant elements in EUCC/CC**) the assurance level is established by the PP.

In general, a higher assurance level means:

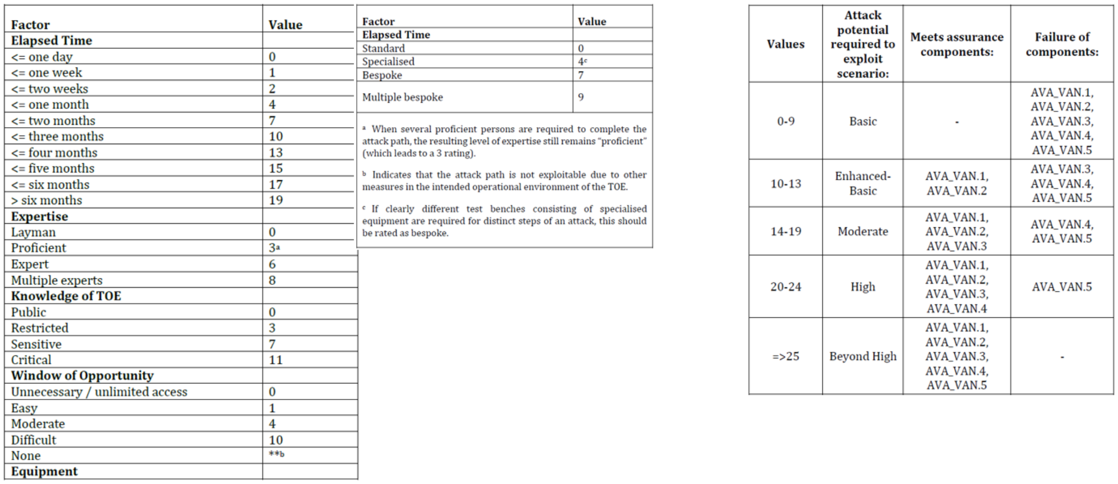
- More assessment activities than in the previous EAL, e.g., by including SARs from additional families.
- Deeper assessment activities than in the previous EAL, e.g., by including hierarchically higher SARs from the same families.

It is also relevant to mention that some SARs (and assurance families in general) can be directly linked with requirements of the CRA associated to manufacturer processes (i.e., user guidance, technical guidance, lifecycle of the product and related procedures, etc.). As such, it's worth enumerating those assurance families:

- **Class AGD: Guidance documents** establishes requirements to be met by **manufacturer's user guidance** on the TOE, with the **AGD_PRE** family (Preparative procedures) scoping requirements for guides related to TOE acceptance, deployment and secure configuration, and **AGD_OPE** (Operational user guidance) family scoping requirements for secure use of the TOE during operational usage.
- **Class ADV: Development** is related to TOE development activities, especially those linked with the design of the TOE. **ADV_TDS** (TOE Design) covers aspects of the documentation of TOE design decomposition (e.g., specification of architectural and functional blocks of the TOE); **ADV_FSP** (Functional specification) establishes requirements for documenting the interfaces of the TOE; **ADV_ARC** (Security Architecture) requires a documented security architecture, e.g., lines of defence that the TOE sets toward protecting from specific typologies of attacks; **ADV_IMP** (Implementation representation) links the design with aspects of the implementation; **ADV_INT** (TSF Internals) requires that the internal design of the TSF is designed in a well-structured manner, so that any changes to the TSF can be added to the implementation with controlled impact; **ADV_SPM** (Formal TSF Model) requires the establishment of a formal security policy for modelling certain security features of the TOE.
- **Class ALC: Life-cycle support** deals with the assurance of a high number of aspects of security during the different phases of the TOE lifecycle. **ALC_CMS** (CM scope) **and ALC_CMC** (CM capabilities) require configuration management to be carried out on the items that are relevant for TOE development (i.e., source code, design documentation), with a number of security controls; **ALC_DEL** (Delivery) establishes security requirements to consider during the delivery of the TOE to end-users, either through physical or digital means; **ALC_DVS** (Development security) scopes the physical, logical and procedural security in the facilities where the TOE is developed and manufactured; **ALC_FLR** (Flaw remediation) requires the manufacturer to perform adequate procedures when security flaw (vulnerability) reports on the TOE are raised; **ALC_LCD** (Life-cycle definition) requires TOE development to follow an established and controlled lifecycle model; **ALC_TAT** (Tools and techniques) requires manufacturer's control over the set of tools used for TOE development and manufacturing.

Moreover, the **AVA_VAN Vulnerability Analysis** family includes requirements for evaluators to conduct vulnerability assessment and penetration testing on the TOE during the evaluation. AVA_VAN includes five hierarchical assurance components (SARs), from AVA_VAN.1 to AVA_VAN.5 that establish different levels of assurance when performing the vulnerability assessment of the TOE. The main difference is that each increasing level of AVA_VAN uses higher ***attack potential*** than the previous one, where the attack potential is a numeric value that determines the effort that an attacker must use to exploit a vulnerability in the TOE, and includes factors such as attacker expertise, available equipment, knowledge of the TOE or time available to perform the attack.

The figure below shows, on the left, of the table presented in [CEM2022] establishing the factors taken into consideration for calculation of the attack potential and, on the right, the relationships between the value of the attack rating and the AVA_VAN levels:



Factor	Value
Elapsed Time	
<= one day	0
<= one week	1
<= two weeks	2
<= one month	4
<= two months	7
<= three months	10
<= four months	13
<= five months	15
<= six months	17
> six months	19
Expertise	
Layman	0
Proficient	3[a]
Expert	6
Multiple experts	8
Knowledge of TOE	
Public	0
Restricted	3
Sensitive	7
Critical	11
Window of Opportunity	
Unnecessary / unlimited access	0
Easy	1
Moderate	4
Difficult	10
None	**[b]
Equipment	

Factor	Value
Elapsed Time	
Standard	0
Specialised	4[c]
Bespoke	7
Multiple bespoke	9

[a] When several proficient persons are required to complete the attack path, the resulting level of expertise still remains "proficient" (which leads to a 3 rating).

[b] Indicates that the attack path is not exploitable due to other measures in the intended operational environment of the TOE.

[c] If clearly different test benches consisting of specialised equipment are required for distinct steps of an attack, this should be rated as bespoke.

Values	Attack potential required to exploit scenario:	Meets assurance components:	Failure of components:
0-9	Basic	-	AVA_VAN.1, AVA_VAN.2, AVA_VAN.3, AVA_VAN.4, AVA_VAN.5
10-13	Enhanced-Basic	AVA_VAN.1, AVA_VAN.2	AVA_VAN.3, AVA_VAN.4, AVA_VAN.5
14-19	Moderate	AVA_VAN.1, AVA_VAN.2, AVA_VAN.3	AVA_VAN.4, AVA_VAN.5
20-24	High	AVA_VAN.1, AVA_VAN.2, AVA_VAN.3, AVA_VAN.4	AVA_VAN.5
=>25	Beyond High	AVA_VAN.1, AVA_VAN.2, AVA_VAN.3, AVA_VAN.4, AVA_VAN.5	-

Figure 12 Calculation of attack potential and attack rating related with AVA_VAN levels

AVA_VAN levels directly relate to the assurance levels established in the CSA, which is of interest for the objective of this study. EUCC relates them as follows:

- **AVA_VAN.1 and AVA_VAN.2** map to assurance level '***substantial'*** of the CSA;
- **AVA_VAN.3 to AVA_VAN.5** map to assurance level '***high'*** of the CSA.

Lastly, CC also allows to define ***Extended SARs,*** through the same extension mechanism used for the SFRs. Therefore, it is possible to define extended assurance components, assurance families or even assurance classes when the evaluation requires including assessment activities not contemplated within the SARs included in [CC2022P3].

4.4. Other relevant elements in EUCC/CC

Within the many elements that exist within the EUCC framework and CC standards, some of them can also be deemed relevant for this study and are briefly introduced in this sub-chapter.

The **Security Target** is the keystone document that manufacturers develop and evaluators assess during EUCC evaluations. The Security Target (ST) is evaluated according to the SARs included in the ASE class, which define key aspects of the evaluation, such as:

- **Defines** and describes the **Target of Evaluation (TOE),** establishing also the physical and logical boundary, drawing a clear delimitation between the TOE and the **operational environment**.
- Specifies the **Security Assurance Requirements (SARs)**, requirements placed on the manufacturer, the evaluation evidence, and the evaluators that define the scope of the assessment activities to be conducted in the evaluation
- Includes the instantiation of the **Security Functional Requirements (SFRs)**, determining the security features that the TOE must implement, that are also under the scope of the evaluation and that are subject of testing.

- Describes the **Security Problem Definition,** which establishes the assets that the TOE must protect, the threats to those assets that the TOE may counter, and the policies based on which the TOE must implement certain security services. It also specifies assumptions on the operational environment required to ensure that the TOE operates as expected. It can be seen as a threat modelling and simplified risk assessment, as will be discussed in section **5.3 Manufacturer risk assessment** of this document.
- When the evaluation claims conformance with a **Protection Profile (PP)**, it lists the PPs to which the ST is conformant, and the form of conformance (exact, strict, demonstrable).

Protection Profiles are documents that establish the main contents of the Security Target used in the evaluation of certain types or categories of ICT products. They establish, among others, the TOE definition, Security Functional Requirements, Security Assurance Requirements and Security Problem Definition (including assets to protect and applicable threats). They set a ST baseline for similar types of products deployed in similar environments and that must provide an equivalent security solution to the same security problem. When STs of different manufacturers and products claim conformance to the same protection profile, the content of these STs differ only in specific product-dependent aspects in the TOE description and in the technical details describing how each TOE implements the SFRs coming from the PP.

Protection Profiles are instantiated in Security Targets through ***Conformance Claims****,* by which the ST declares conformity with one or more PPs. There may be some flexibility regarding how a ST follows the contents of the PP, which depends on the type of **PP conformance**:

- ***Strict*** **conformance**: the security problem, SFRs and SARs can be equivalent or a superset of those in the PP. For example, new elements (assets, threats, policies) can be added in the Security Problem Definition, or additional SFRs or SARs can be included in the compliant ST.
- *Strict + demonstrable****:*** the security problem, SFRs and SARs can be more restrictive than those in the PP, i.e., allowing to replace elements of the SPD in the PP or SFRs/SAR of the PP by others if it can be demonstrated that they are equivalent or more restrictive than those in the PP.
- *Exact conformance:* the security problem, SFRs and SARs need to be *identical* to those in the PP (therefore no flexibility is offered to add, remove or modify these elements).

The use of protection profiles is very frequent in the CC/EUCC certification landscape and in the last 5 years 74% of the CC certifications have been conducting using a PP[8].. It is also quite common that PPs define extended SFRs and/or SARs that aren't included in the CC standard and that fit well for certain security aspects inherent to the type of product covered by the PP. Doing so permits to include such extended functionality within the scope of the evaluation.

All PPs need to undergo EUCC/CC certification before they can be approved and used in STs. PPs are often elaborated by private industry entities, e.g. EUROSMART or GlobalPlatform, by SDOs, e.g. ETSI or CEN/CENELEC, or by public entities such as public entities at national level, such as National Certification Schemes, such as ANSSI or BSI. The list of the currently certified protection profiles can be found in https://commoncriteriaportal.org website.

A **Collaborative Protection Profile (cPP)** is a type of Protection Profile created through a collaborative process. By involving industry engagement, cPPs aim to define better security requirements and testing methodologies. These profiles are developed by International Technical Communities (iTCs),

[8] According to jtsec's statistics: https://www.jtsec.es/files/2022%20CC%20Statistics%20Report.pdf

consisting of CC and technology experts, and sponsored by at least two CCRA nations. Collaborative PPs often include Supporting Documents that, for example, the specific assurance activities for the SFRs and SARs of the cPP.

Unlike product certificates, PP certificates don't expire after a given timeframe. However, the stakeholders responsible for their maintenance tend to periodically update them as a response to changes in the technological or regulatory landscape. Moreover, when a new version of the CC standard is published, it is often accompanied by a transition period after which the use of CC based on the previous version of CC is no longer permitted. Therefore, updates in the CC standard indirectly push the update of PPs certified under the previous version, leading to a new PP certification process. At the date of publication of this report, the industry is transitioning from Common Criteria version 3.1, revision 5 to Common Criteria 2022 revision 1. The policy regulating this transition[9] establishes that:

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

Evaluation evidence refers to those inputs that manufacturers must provide to the Information Technology Security Evaluation Facility (ITSEF) as input for the evaluation. They are mainly the TOE itself and the evaluation evidence required by the SARs included in the ST (e.g., the ST itself, user guidance, design documentation, etc), but the set of evidence varies depending on the SARs included in the evaluation. For example, in EAL4 or above the manufacturer needs to provide the implementation representation (source code for SW or FW, or RTL code for HW), but for evaluations using EAL3 or lower these elements are not provided to the ITSEF.

Dependencies between SFRs and between SARs are established in [CC2022P2] and [CC2022P3] respectively. This means that including a SFR in the ST also requires including those SFRs on which the former depends, and in turn also requires the inclusion of any SFRs dependent on the latter, setting up a chain of dependencies. This is also applicable to SARs included in the ST and their dependencies. For example, SFRs related to generation of audit records can depend on those related to generation of timestamps, as the audit logs need to be accompanied by a reliable timestamp. In the case of SARs, activities related to examination of the TOE interfaces can depend on those requiring a certain level of detail in the documentation of the TOE design. The CC standard allows, in certain cases, to not include dependent SFRs or SARs subject to an adequate justification. Sections **5.1** and **5.2** of this document discuss how Security Functional Requirements (SFRs) and Security Assurance Requirements (SARs) can be utilized for EUCC certification to meet security requirements that could be equivalent to those outlined by the CRA essential security requirements (ESRs). In these instances, using CC SFRs and/or SARs to satisfy CRA ESRs in a future EUCC certifications would require including in it the dependent CC SFRs and/or SARs as well.

Technical Mechanism for Patch Management: EUCC will include the possibility for manufacturers to include in the scope of the EUCC evaluation, and therefore provide a description of, a technical mechanism that allows the TOE to receive and install updates on the certified product. The patch

[9] https://commoncriteriaportal.org/files/ccfiles/CC2022CEM2022TransitionPolicy.pdf

management procedure, including the mechanism as implemented into the ICT product by the applicant for certification, can be used after the certification of the ICT product under the responsibility of the CAB. The technical mechanisms part of the Patch Management refers specifically to those mechanisms and functions for the adoption of the patch into the ICT product.

EUCC will not oblige manufacturers to implement the technical mechanism for patch management through specific SFRs or SARs. It only establishes high level directives that don’t include any details on the implementation of the mechanism or on the evaluation methodology that ITSEF shall follow for such patch management. However, at the date of publication of this report industry is starting to adopt the “ISO/IEC CD TS 9569 Information security, cybersecurity and privacy protection — Evaluation criteria for IT security — Patch Management Extension for the ISO/IEC 15408 series and ISO/IEC 18045” [ISO_TS_9569]. This Technical Specification addresses the gap in the CC standard regarding the evaluation of IT products post-patch application, including extended SARs that define methodologies for assessing the security of updated products, and SFRs that describe the mechanism that ICT products shall implement for obtaining and installing patches.

This study takes [ISO_TS_9569] as a reference proposal for the implementation of a patch management mechanism on the ICT product and to develop associated procedures by the manufacturer, as well as for CABs to conduct assessment of both through the methodology defined in that TS.

5. Meeting CRA requirements through EUCC certifications

Section 4 Relevant EUCC concepts for this study introduces the EUCC and CC elements that include technical details and other factors to consider when evaluating how EUCC certifications will meet the CRA requirements. This section aims to analyse the aspects of the CRA that are relevant for demonstrating conformity, and hence would need to be addressed by certification on the basis of the EUCC.

As previously indicated in section 2.3 Background, the analysis performed in this report seeks to examine the technical aspect involved in the implementation of the CRA through EUCC and provides potential conclusions that could be considered by the European Commission when establishing presumption of conformity, but this study should not be read as providing guidelines for establishing it. Please, refer to the aforementioned section for full background information on the possibility of presumption of conformity as established in the CRA.

The analysis presented in this section considers the following aspects as the key ones for the implementation of CRA through EUCC and its technical elements:

1. **CRA Annex I essential cybersecurity requirements, Part I: Security requirements relating to the properties of products with digital elements.** It needs to be explored how the SFRs describing the security functionality of the product under the scope of EUCC evaluation may serve to demonstrate that the TOE also meets those CRA essential cybersecurity requirements in Annex I, part I, defining requirements relating to the properties of products with digital elements.
2. **CRA Annex I essential cybersecurity requirements, Part II: Vulnerability handling requirements.** It needs to be explored how the SARs in the EUCC evaluation involving assessment activities performed by the EUCC CAB on the TOE itself and on the manufacturer's documentation and procedures, can also demonstrate compliance with those essential cybersecurity requirements in CRA Annex I, part II, expressing vulnerability handling requirements for products with digital element.
3. **CRA Risk assessment:** How the risk assessment required by CRA (as per CRA Annex I, Part I, 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;")* for manufacturers of products with digital elements can be covered by the threat modelling of the EUCC that ultimately lead to the selection of SFRs included in the EUCC evaluation. This link is established through the relationship between ESRs in CRA and SFRs in EUCC, as described in point (1) above.
4. **Scope of the TOE under EUCC:** How, and under which scenarios, the scope of the TOE under EUCC corresponds with the scope of the product with digital elements of the CRA with their integrated remote data processing solutions. In order to ensure that the full product meets with the CRA essential cybersecurity requirements, the scope of the EUCC TOE should be, in principle, equivalent to that of the product with digital elements.

This chapter addresses in the following sub-sections respectively these four topics. It must be noted that other topics such as coverage of manufacturer obligations related to CRA Annex II (Information and Instructions to the User) and Annex VII (Contents of the Technical Documentation), or strategies on how to comply with the CRA essential Requirements through EUCC certification cases existing in the industry are covered separately in chapters 6 Analysis of the EUCC certification landscape for Critical and Important products and 7 Strategies for implementation in the industry.

5.1. Complying with CRA ESRs Annex I, Part I through EUCC technical elements

The essential cybersecurity security requirements in CRA Annex I.1 describe requirements in the form of security functionalities to be implemented in the product with digital elements. As such, they describe security functions that are in many cases equivalent to those in the CC SFRs to be used in EUCC, which are meant to be met by the TOE.

In EUCC evaluations, manufacturers will include in the EUCC Security Target a number of SFRs that correspond to the security functionalities claimed for the TOE. As explained above, these can be SFRs defined by the standard in [CC2022P2] or they can be extended components designed by the author of the ST or the Protection Profile. The activities that CABs will conduct in relation to the SFRs during an EUCC evaluation can be summarized as follows:

- Documentary verification of the correctness and consistency of the SFRs written in the ST in accordance with the rules defined in the CC standard. Depending on the chosen EAL, this can include additional verifications of the instantiation of the SFRs in the TOE design documentation or of the coverage of the SFRs in the TOE test plans.
- Verification that the security features described in the SFRs are correctly implemented by the TOE.
- Vulnerability assessment and penetration testing in search of exploitable vulnerabilities in the TOE. The effort expended in trying to exploit potential vulnerabilities is dependent on the of AVA_VAN level aimed for.

Thus, using the CC methodology in the context of an EUCC evaluation CABs will verify that the relevant Security Functional Requirements are met.

Based on this analysis, this study considers that, when the security functionality described by ESRs in Annex I Part I of the CRA is equivalent to that described by SFRs in a EUCC certification, and it is demonstrated within the context of the EUCC evaluation that such requirements are met by the certified product, then this situation can be assumed as also meeting the CRA ESRs.

Disclaimer

With regards to presumption of conformity, CRA Article 27 establishes in point (1) that "*The Commission shall, in accordance with Article 10(1) of Regulation (EU) No 1025/2012, request one or more European* ***standardisation organisations to draft harmonised standards*** *for* ***the essential cybersecurity requirements set out in Annex I to this Regulation****.*" It also establishes in point (2) that "The Commission may adopt **implementing acts** establishing **common specifications covering technical requirements that provide a means to comply with the essential cybersecurity requirements** set out in Annex I for products with digital elements that fall within the scope of this Regulation."

At the date of publication of this report, such standardization work has been initiated[10], but no harmonized standards exist yet, and no common specifications describing technical means to comply with the CRA essential requirements exist so far.

[10] see draft Commission standardisation request available at : https://ec.europa.eu/docsroom/documents/58974

This study aims to establish equivalence or mappings between the CRA essential security requirements (ESRs) and EUCC Security Functional Requirements (SFRs). To achieve this, the section evaluates the CRA's essential security requirements based on their current legal text, prior to the availability of common standards and specifications. When equivalence is established between CRA ESRs and CC SFRs, it will be based on the assumption that the SFRs correspond to product security functionalities equivalent to those described by the ESRs in Annex I Part I of the CRA, without considering any future harmonized standards or common specifications that may provide more detailed technical requirements. In the same way, the results of the mapping in this study should not be interpreted as providing any final response to the notion of coverage of essential requirements in the legal meaning of Article 27.

Additionally, horizontal standards developed for the CRA will further impact the analysis. Once available, this report may be revised to assess whether these standards should be referenced in Security Target (ST) and Protection Profile (PP) documents, thereby complementing the SFRs that have been extended or adapted for the CRA's ESRs, such as those related to data minimization.

Consequently, this study may require updates to incorporate future developments from the standardization work referenced in Article 27 of the CRA.

The analysis of equivalence between CRA ESRs and CC SFRs to be used in EUCC is presented in-detail in the Annex **"1 ANNEX I. Mapping the CRA Requirements for EUCC certification process (detailed analysis)"** of this document. Due to the nature of some ESRs in the CRA Annex I, part I, which don't directly describe functional security features of the product, it may not be possible to find SFRs in EUCC that describe equivalent security functionality. However, it is possible to use EUCC SARs that aim to assess the manufacturer's procedures to cover those requirements in the CRA ESRs.

The results of this analysis are summarized in the table below:

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

			case is when the SPD in the ST declares an assumption for trusted administrators, ensuring that when they receive the TOE, they shall perform a secure initial configuration following the AGD_PRE.1 (Preparative Procedures) guidance. **Note:** this option is quite common in CC evaluations and could be used in most cases.
(2)(c) *ensure that vulnerabilities can be addressed through security updates, including, where applicable, through automatic security updates that are installed within an appropriate timeframe enabled as a default setting, with a clear and easy-to-use opt-out mechanism, through the notification of available updates to users, and the option to temporarily postpone them;*	SFRs implementing the (technical) patch mechanism involved in EUCC's patch management procedure **including or refined to include** the technical mechanism referred in [EUCC] IV.4 Patch management (4)(b): a. Automatic updates enabled by default with installation of updates after a timeframe. b. An option to disable automatic updates. c. Notification of available updates to users. d. An option to temporary postpone the updates to be installed when the automatic updates setting is enabled.	SARs implementing the patch management procedure, in the set of evaluation activities referred in [EUCC] IV.4 Patch management (4)(c): specific evaluation activities to assess during the EUCC evaluation the points (a), (b), (c) and (d) referred in the previous column.	This study chooses to set specific constraints on the patch management that will be adopted under EUCC rather than providing separate components. This study hasn't performed a detailed technical analysis on how to develop the SFRs and SARs linked to the described mechanism. It is expected that technical specifications will be available to describe the mechanism in compliance with this CRA ESR. As an alternative, the ST author can design extended SFRs that, either alone or in combination with others, model the security functionality expressed by this ESR.
(2)(d) *ensure protection from unauthorised access by appropriate control mechanisms, including but not limited to authentication, identity or access management systems, and report on possible unauthorised access;*	For **identification and authentication**: FIA_UID.1 Timing of identification or FIA_UID.2 User identification before any action, and FIA_UAU.1 Timing of authentication or FIA_UAU.2 User authentication before any action		Access management could be modelled with ad-hoc extended SFRs rather than with the generic FDP_ACC.1 Subset access control and FDP_ACF.1 User authentication before any action For report on unauthorised access, FAU_GEN.1 Audit data generation shall indicate that the TOE

	For **access management**: FDP_ACC.1 Subset access control, FDP_ACF.1 Security attribute-based access control For **report on possible unauthorised access:** FAU_GEN.1 Audit data generation and one of: a) FAU_SAA.1 Potential violation analysis b) FAU_STG.1 Audit data storage location		generates audit records on such events, combined with **one of:** a) FAU_SAA.1 Potential violation analysis shall have filled the assignment in this SFR in order to indicate the events and rules that would mean a possible unauthorised access event, when this functionality is implemented in the TOE. b) FAU_STG.1 selecting the option of sending audit records to an external IT entity, if the audit data is aggregated on another device for potential violation analysis.
(2)(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;*	**Confidentiality of stored data through <u>one or more</u> techniques/SFRs**: • FDP_SDC.1 • FCS_COP.1 implementing memory encryption. • FDP_ACC.1 + FDP_ACF.1, and/or FDP_IFC.1 + FDP_IFF.1 for access control to memories or information flow control for stored data. • FPT_PHP.3 and/or FDP_ITT.1 and/or FPT_ITT.1 for protection against physical attacks and tampering (when attackers can physically access the TOE in high-assurance scenarios). **Confidentiality of communications**:		For different communication channels, a different instance of the SFRs related to confidentiality of communications shall be added. For each different cryptographic mechanisms used for protection of confidentiality, different instances of FCS_COP.1 need to be added. Other extended components used by industry can also ensure protection of communications, such as FCS_HTTPS_EXT.1, FCS_HTTPS_EXT.2 for HTTPS (from [PP_APPSW] or for TLS and DTLS, FCS_TLSC_EXT.1, FCS_TLSS_EXT.1. or FCS_DTLSC_EXT.1, FCS_DTLSS_EXT.1 from [PPFP_TLS].

	FTP_ITC.1 Import of user data without security attributes (between TOE and other IT entities), FTP_TRP.1 Trusted path (between the TOE and users) For **cryptographic mechanisms** used for the implementation any of the above protections: FCS_COP.1 Cryptographic operation		
(2)(f) *protect the integrity of stored, transmitted or otherwise processed data, personal or other, commands, programs and configuration against any manipulation or modification not authorised by the user, and report on corruptions;*	**Integrity of data at rest and reporting corruption:** either FDP_SDI.1 +FAU_GEN.1 Audit data generation (registering event for corruption of data) or FDP_SDI.2 **Integrity of communications:** FTP_ITC.1 Inter-TSF trusted channel (between TOE and other IT entities), FTP_TRP.1 Trusted path (between the TOE and users) For **cryptographic mechanisms** used for the implementation of any of the above protections: FCS_COP.1 Cryptographic operation For **particular reporting of integrity violation** in each communication channel, FAU_GEN.1 Audit data generation.		For different communication channels, a different instance of the SFRs related to confidentiality of communications shall be added. For each different cryptographic mechanisms used for protection of confidentiality, different instances of FCS_COP.1 need to be added. Other extended components used by industry can also ensure protection of communications, such as FCS_HTTPS_EXT.1, FCS_HTTPS_EXT.2 for HTTPS (from [PP_APPSW] or for TLS and DTLS, FCS_TLSC_EXT.1, FCS_TLSS_EXT.1. or FCS_DTLSC_EXT.1, FCS_DTLSS_EXT.1 from [PPFP_TLS].
(2)(g) process *only data, personal or other, that are adequate, relevant*		ADV_PDM.1: Processed Data	

and limited to what is necessary in relation to the intended purpose of the product with digital elements (minimisation of data);		Minimisation (Extended)	
(2)(h) protect *the availability of essential and basic functions, also after an incident, including through resilience and mitigation measures against denial-of-service attacks;*	FRU_FLT.1 Degraded fault tolerance FPT_FLS.1 Failure with preservation of secure state		Note: it must be acknowledged that this ESR depicts and addresses a threat scenario that could be very specific, for example due to DoS attacks being not applicable to a wide variety of IT systems. As such, the ST author must consider that this ESR might be deemed as not applicable on the basis of the corresponding risk assessment and, therefore, the proposed SFRs wouldn't be needed in the EUCC evaluation.
(2)(i) minimise *the negative impact by the products themselves or connected devices on the availability of services provided by other devices or networks;*	For minimization of impact by the **product itself:** FPT_INI.1 TSF initialization FPT_TST.1 TSF Testing For minimization of impact by **connected devices**: FDP_IFC.1 Subset information flow control FDP_IFF.1 Simple security attributes		The author of this report understands that this ESR has to distinguishable parts: a) Minimisation of the negative impact **by the product itself** on the availability of services provided by other devices or networks. b) Minimisation of the negative impact **by other connected devices** (different from the product itself) on the availability of services provided by other devices or networks. For the first part, the selected SFRs FPT_INI.1 TSF initialization and FPT_TST.1 TSF Testing can mitigate the impact of the product itself. For the second part, this capability is relevant in those products whose intended purpose is to control the communications of other devices in the network by filtering network traffic or limiting its

			rate. Some examples could be firewalls or IPS devices. For those specific cases, this study recommends taking the specific SFRs for DoS protection in the network, e.g.: • For Firewalls, FFW_RUL_EXT.1 Stateful Traffic Filtering in [CPP_FW] • For IPS, those under IPS class in [PPMOD_IPS]
(2)(j) be *designed, developed and produced to limit attack surfaces, including external interfaces;*		AVA_VAN.1 Vulnerability survey ADV_FSP.1 Basic functional specification AGD_OPE.1 Operational user guidance	
(2)(k) be *designed, developed and produced to reduce the impact of an incident using appropriate exploitation mitigation mechanisms and techniques;*	FPT_FLS.1 Failure with preservation of secure state FPT_RCV.1 Manual recovery	ADV_ARC.1 Security architecture description ADV_TDS.1 Basic design ADV_FSP.1 Basic functional specification	Note: the security functionalities needed by FPT_FLS.1 and FPT_RCV.1 are specific for certain threat scenarios and IT systems, and could not be required in the general case. The manufacturer risk analysis shall assess where the implementation of those security functions is actually necessary in order to meet this ESR.
(2)(l) provide *security related information by recording and monitoring relevant internal activity, including the access to or modification of data, services or*	FAU_GEN.1 Audit data generation FMT_SMF.1 Specification of Management Functions FMT_SMR.1 Security roles		In FAU_GEN.1 Audit data generation it shall be indicated what events shall be logged. In FMT_SMF.1, the opt-out mechanism (enable/disable audit function) shall be included.

functions, with an opt-out mechanism for the user;			
(2)(m) *provide the possibility for users to securely and easily remove on a permanent basis all data and settings and, where such data can be transferred to other products or systems, ensure that this is done in a secure manner.*	**For removal of data/settings:** FMT_SMF.1 Specification (with a function to delete data/settings) FDP_RIP.1 Subset residual information protection **For transferring data/settings:** FMT_SMF.1 Specification (with a function to transfer data/settings) FDP_ETC.1 Export of user data without security attributes or FDP_ETC.2 Export of user data with security attributes FTP_ITC.1 Inter-TSF trusted channel		For removal of data, other extended SFRs than the ones proposed here could also meet the ESR. For example, in the CC industry it's possible to find "FPT_WIPE_EXT.1 Data Wiping" from [CPP_HARDCOPY], valid for the context and type of TOE in that PP. Alternatively, a "Factory Reset" functionality could provide equivalent functionality in certain cases.

Table 1 Coverage of Annex I.I ESRs

The following notes should be considered when reading the above table:

(1) When **more than one** CC SFRs or SARs are identified as meeting a CRA ESR, then **all** of those SFRs/SARs will need to be included in the EUCC evaluation in order to fully meet the related CRA ESR.

(2) Those SFRs or SARs tagged with the keyword ***Extended*** don't exist in [CC2022P2] or [CC2022P3] and this study proposes designing extended SFRs / SARs that both follow the rules of the CC standard and presents a security requirement covering fully or partially the related CRA ESR.

(3) Each SFR or SAR in the proposed list can be replaced by **hierarchically higher** SFRs/SARs in the same family as the proposed one.

(4) The **dependencies** of the SFRs/SARs proposed as covering the ESRs **have not been included** in the above table. The author of the ST is responsible for including the dependencies established for each SFR/SAR in [CC2022P2], [CC2022P3] or in the definition of the extended component, or otherwise provide a justification on why the dependencies are not needed for their particular ST.

(5) The mappings provided in the above table are a **proposal**. Common Criteria could allow combinations of other SFRs or definition of alternative extended SFRs/SARs that could potentially describe the same security functionality. The proposal here included is extracted from a preliminary investigation.

(6) The mapping goes through and covers all the ESRs from Annex I part I of CRA, however the CRA allows manufacturers, through the risk assessment, to justify that some of the ESRs are not required for their particular product with digital elements. In such cases it will be possible to exclude the mentioned SFR from the EUCC evaluation.

5.2. Complying with ESRs in CRA Annex I, Part II through EUCC technical elements

The essential requirements included in Annex I, Part II describe requirements related to vulnerability handling of products with digital elements. This study proposes a series of SARs used to model security considerations of the EUCC security evaluation that can be mapped to ESRs in CRA Annex I, Part II, as they describe similar security aspects.

The SARs that will be included in an EUCC evaluation are determined either by the protection profile used, if any, or through a manufacturer's decision based on aspects such as the assurance level required for a particular product under evaluation, which will depend on the criticality of the assets protected by it, or the degree of exposure to attack scenarios. As mentioned in previous sections, it will be possible to include SARs in EUCC evaluations through assurance packages, from EAL1 to EAL7, that are expected to determine the evaluation activities that will be included as part of the evaluation. These activities themselves place requirements belonging to certain assurance classes on the manufacturers of the product under evaluation.

In EUCC evaluations, CABs will carry out certain verification or assessment activities determined by the SARs and by the CC methodology ([CEM2022]) in order to determine that manufacturers meet the requirements (procedural, documentary, etc.) required by the SARs. In such way, if an equivalence relationship can be determined between SARs in the EUCC evaluation and the ESRs in CRA Annex I, Part II, it is possible to conclude that the demonstration of compliance with a SAR during the EUCC evaluation means that the equivalent ESR is met as well.

Disclaimer:

As already stated in section **5.1 Complying with CRA ESRs Annex I, Part I through EUCC technical elements**, this study establishes equivalence between ESRs in Annex I and SFRs/SARs taking into account their formulation as is currently in the CRA, and without considering future outputs standardisation work as per CRA Article 27. Please, refer to the aforementioned section for further information.

The in-detail analysis of equivalence between CRA ESRs and SARs is presented in-detail in the annex **"3. Annex III. EUCC CABs and conformity assessment"** of this document. The results of the analysis are summarized in the table below:

Essential security requirement (CRA Annex I part II)	SAR in EUCC/CC or Extended SAR	Notes
Manufacturers of products with digital elements shall:	-	-
(1) *identify and document vulnerabilities and components contained in products with digital elements, including by drawing up a software bill of materials in a commonly used and machine-readable format covering at the very least the top-level dependencies of the products;*	ALC_FLR.1 Basic flaw remediation ALC_SBM.1: Software bill of materials (Extended)	
(2) *in relation to the risks posed to products with digital elements, address and remediate vulnerabilities without delay, including by providing security updates; where technically feasible, new security updates shall be provided separately from functionality updates;*	**Either one of:** - ALC_FLR.1 Basic flaw remediation + SARs implementing the (technical) patch mechanism involved in EUCC's patch management procedure (this study proposes to use those in [ISO_TS_9569]). -ALC_FLR.3 Flaw reporting procedures **and** ALC_FLR.4 Flaw remediation with distinction between security and functional flaws (Extended).	
(3) *apply effective and regular tests and reviews of the security of the product with digital elements;*	ALC_PSR.1 Periodic security review and testing	
(4) *once a security update has been made available, share and publicly disclose information about fixed vulnerabilities, including a description of the vulnerabilities, information allowing users to identify the product with digital elements affected, the impacts of the vulnerabilities, their severity and clear and accessible information helping users to remediate*	ALC_FLR.1 Basic flaw remediation	The coverage of this CRA ESR by the SARs identified here doesn't consider the possibility of not publishing vulnerability information until certain user-base has already patched. The general case considers that it will be published.

the vulnerabilities; in duly justified cases, where manufacturers consider the security risks of publication to outweigh the security benefits, they may delay making public information regarding a fixed vulnerability until after users have been given the possibility to apply the relevant patch;		Further guidance might be developed under the CRA to further define the use cases where it is justified to exceptionally wait before releasing the information. Moreover, the rules in the EUCC could be updated accordingly.
(5) *put in place and enforce a policy on coordinated vulnerability disclosure;*	N/A	This requirement can be covered by [EUCC] Article 8, point 6b requires the manufacturer to provide to the CAB “a description of the applicant’s vulnerability management and vulnerability disclosure procedures.”.
(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;*	ALC_FLR.2 Flaw reporting procedures	Also covered in EUCC Article 33.2 “*2. The holder of an EUCC certificate shall maintain and publish appropriate methods for receiving information on vulnerabilities related to their products from external sources, including users, certification bodies and security researchers.”*
(7) p*rovide 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;*	**Either one of:** - ALC_FLR.1 Basic flaw remediation + SARs implementing the (technical) patch mechanism involved in the EUCC patch management procedure (this study proposes to use those in [ISO_TS_9569]). -ALC_FLR.3 Systematic flaw remediation **and** ALC_FLR.4 Flaw remediation with distinction between security and functional flaws (Extended).	

(8) *ensure that, where security updates are available to address identified security issues, they are disseminated without delay and, unless otherwise agreed between a manufacturer and a business user in relation to a tailor-made product with digital elements, free of charge, accompanied by advisory messages providing users with the relevant information, including on potential action to be taken.*	**Either one of:** - ALC_FLR.1 Basic flaw remediation + SARs implementing the (technical) patch mechanism involved in the EUCC patch management procedure **refined for automatic installation of patches as in ESR (2)(c) of ESR Annex I, part 1.** -ALC_FLR.3 Systematic flaw remediation	The non-functional part of the ESR refers to the free-of-charge nature of updates. This aspect refers more to a commercial agreement topic. In the current version of EUCC Implementing Act, no technical elements exist that address this type of issue, and the extension mechanism present in the Common Criteria standard is meant to address cybersecurity-related requirements and others related to other aspects like revision of legal contracts in an effective manner. The interpretation of this CRA essential requirement is that the manufacturer could sign a statement of the free of charge updates when applying to certification, whose presence should be controlled by the CAB, and further verified under the conditions of market surveillance. The EUCC scheme could be supported by a template for application that provide the statement to be signed and define who should sign it.

Table 2 Coverage of ESRs in Annex I.II

The following notes should be considered when reading the above table:

(1) When **more than one** CC SAR is identified as meeting a CRA ESR, then **all** of those SARs will need to be included in the EUCC evaluation in order to fully meet the related ESR.

(2) Those SARs tagged with the keyword ***Extended*** don't exist in [CC2022P3] and this study proposes designing extended SARs that both follow the rules of the CC standard and presents a security requirement covering fully or partially the related CRA ESR.

(3) Each SAR in the proposed list can be replaced by **hierarchically higher** SARs in the same family as the proposed one.

(4) The **dependencies** of the SARs proposed as covering the ESRs **have not been included** in the above table. The author of the ST is responsible for including the dependencies established for each SAR in [CC2022P3] or in the definition of the extended component, or otherwise provide a justification on why the dependencies are not needed for their particular ST.

(5) The mappings provided in the above table are a **proposal**. Common Criteria could allow combinations of other SARs or definition of alternative extended SARs that could potentially describe the same security functionality. The proposal here included is extracted from a preliminary investigation.

(6) The mapping goes through and covers all the ESRs from Annex I part I of CRA, however for the CRA allows manufacturers through the risk assessment to justify that some of the ESRs aren't required for their particular product with digital elements. In such cases, it will be possible to exclude the mentioned SAR from the EUCC evaluation.

5.3. Manufacturer risk assessment

The CRA establishes in Article 13 that, when placing a product with digital elements on the market, the manufacturer shall include a cybersecurity risk assessment referred to in the technical documentation required pursuant to CRA Article 31 and Annex VII. Article 13 (3) states that the cybersecurity risk assessment shall comprise at least an analysis of cybersecurity risks based on the purpose and reasonably foreseeable use, as well as the conditions of use, of the product with digital elements, such as the operational environment or the assets to be protected, taking into account the length of time the product is expected to be in use.

In addition, the same article requires that the cybersecurity risk assessment indicates **"whether and, if so in what manner, the security requirements set out in Annex I, Part I, point (3)**[11]*, are applicable to the relevant product with digital elements and how those requirements are implemented as informed by the cybersecurity risk assessment. It shall also indicate how the manufacturer is to apply Annex I, Part I, point (1), and the vulnerability handling requirements set out in Annex I, Part II*."

The previous sub-sections concluded that CRA ESRs can be complied with in EUCC through SFRs and SARs that express equivalent requirements. In the same way that, as per CRA Article 13, ESRs in Annex I part 1 are deemed to be applicable or not by the manufacturer based on the result of a risk assessment, in EUCC SFRs and SARs also result from a process that starts with the assessment of the risks posed to the assets protected by the EUCC TOE in its intended environment.

The concept within CC that most closely aligns with CRA risk assessment is the Security Problem Definition (**4.4 Other relevant elements in EUCC/CC**). It is based on key concepts such as assets to be protected, threats to those assets, organisational security policies and assumptions for the operational environment of the TOE.

In the CC Security Problem Definition (SPD), the manufacturer identifies the ICT assets that need to be protected by the TOE (e.g., information that is stored, processed, and transmitted) from threats that would impact their security or decrease their value. Threats are defined in terms of an adverse action performed by a threat agent (e.g., an attacker) on assets, with impact on the asset security, e.g., its confidentiality. A typical threat could consist in a remote attacker that eavesdrops on TOE communication on the network, thereby threatening the confidentiality of the data transferred over the network.

The SPD also considers the intended use of the product in its operational environment and, as such, it allows the overall security solution to leverage certain aspects that are provided by the environment and not the TOE itself. This is formally done in CC Security Targets by defining assumptions of the operational environment, considered as axiomatic, in areas that impact security. For example, a classical assumption would be that the administrators of the TOE are well-intentioned, trustworthy, well-trained and that they follow the security policies of the organization in which the TOE is deployed, as well as the security guidance of the TOE. Another example would be that the TOE will be installed

[11] This quoted text from CRA seems inconsistent as, in the version of the CRA available at the date of issuance of this report, the ESRs dependent on the result of the manufacturer's risk assessment are listed under Annex I, Part I, point (2).

in an environment providing physical protection, preventing possible attack paths that involve physical access to the TOE.

It must be noted that, in the context of the manufacturer's risk assessment the CRA doesn't refer to "intended use" but to "intended purpose" and "reasonably foreseeable use". The CRA defines these concepts as follows:

- *'intended purpose' means the use for which a product with digital elements is intended by the manufacturer, including the specific context and conditions of use, as specified in the information supplied by the manufacturer in the instructions for use, promotional or sales materials and statements, as well as in the technical documentation;*
- *'reasonably foreseeable use' means use that is not necessarily the intended purpose supplied by the manufacturer in the instructions for use, promotional or sales materials and statements, as well as in the technical documentation, but which is likely to result from reasonably foreseeable human behaviour or technical operations or interactions;*

The mentions to "intended use" made in this chapter and in other chapters in the context of the discussion of CC technical elements can be seen in a simplified manner as the "intended purpose" defined in CRA, whereas the "reasonably foreseeable use" is different but also contemplated in CC as that situation resulting from the usage of the product in its operational environment by users that follow the TOE user guidance and that align with the security policies of the organisation in which the TOE is deployed.

Another base element of the SPD is the concept of *organisational security policies (OSP)*. These are security rules, procedures, or guidelines imposed in the operational environment. For instance, manufacturers falling under the NIS2 Directive[12] have to implement cybersecurity risk-management measures. These rules, procedures our guidelines can be made by an organization controlling the operational environment of the TOE, or they can be made by legislative or regulatory bodies. OSPs can apply to the TOE and/or the operational environment of the TOE. They can also be used as a way to mitigate the threats to the assets protected by the TOE.

The general model of CC [CC2022P1] considers the Security Problem definition as an axiomatic input to the Security Target and, normally, it would be the result of a previous risk analysis. Figure 1 in [CC2022P1] illustrates these concepts:

[12] https://eur-lex.europa.eu/eli/dir/2022/2555

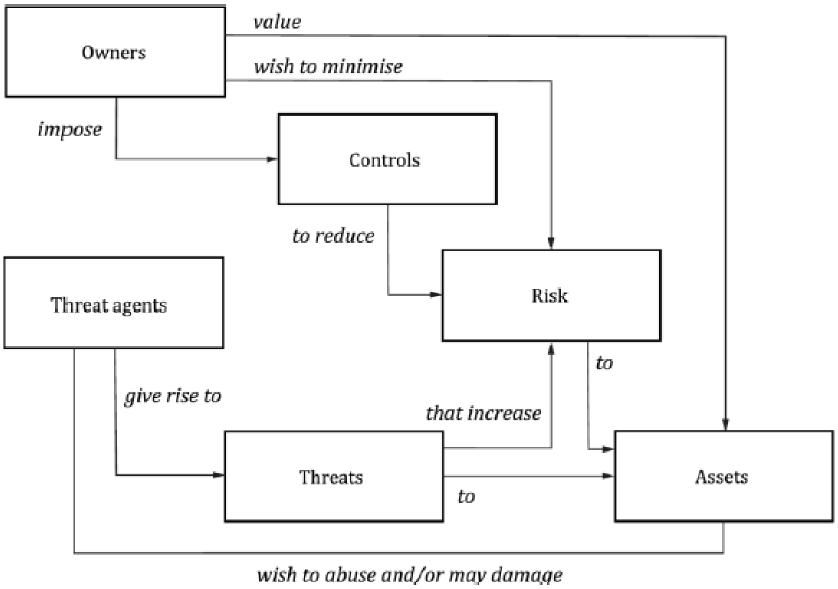


Figure 13: thread and risk model in CC

The definition of threats and assets in the security target leads to the definition of security objectives. There are two types of security objectives:

- *Security objectives for the TOE*: they need to be implemented by the product under evaluation, and they are described in a quite generic way. They ultimately aim to counter threats to the assets, e.g., through security mechanisms implemented in the TOE, or to implement organizational security policies, e.g., by providing a security service that doesn't directly address any threat.

- *Security objectives for the operational environment*: they aim to ensure that the operational environment is able to uphold the assumptions of the SPD (e.g., the operational environment shall ensure that the TOE is installed in a physically protected location), to mitigate a threat (e.g., a secure hardware platform preventing downgrading TOE features), or also implement organizational security policies.

The figure below, taken from [CC2022P1], provides a visual representation of the whole security problem and the relationships with the security objectives for the TOE and for the operational environment.

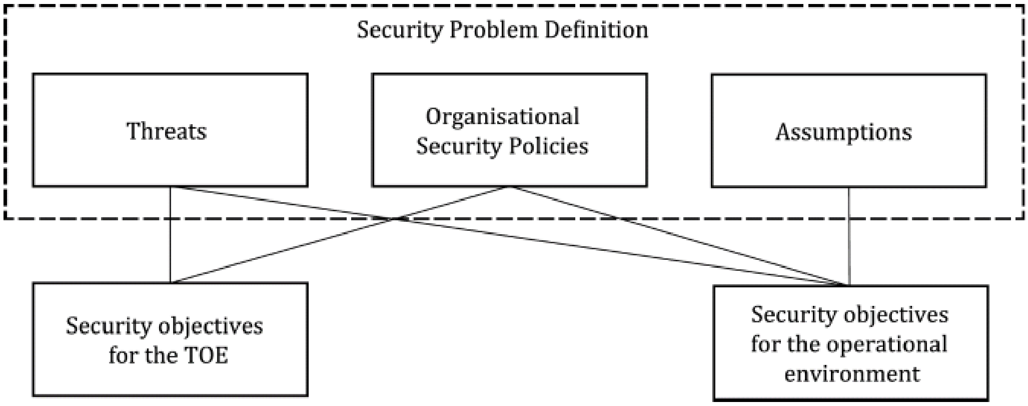

Security Problem Definition
Threats
Organisational Security Policies
Assumptions
Security objectives for the TOE
Security objectives for the operational environment

Figure 14: Relationships between Security Problem Definition and Security Objectives in CC

Ultimately, the security objectives for the TOE need to be met by security functionality implemented in TOE, in other words, SFRs. These will describe the security services and mechanisms implemented by the product to meet the objectives which mean countering the threats.

It must be acknowledged, however, that for SFRs describing a security service rather than a security mechanism, intended to meet a security objective for the TOE that solely implements an organizational security policy it must be carefully considered if they can be used to comply with any of the applicable CRA ESRs. It may not always be possible to justify that those policies and SFRs are connected to any threats or risks identified in the manufacturer's risk analysis and cover relevant ESRs.

The definition of the security problem, the security objectives and threats are included in the assurance families ASE_SPD (Security problem definition), ASE_OBJ (Security objectives) and ASE_REQ (Security requirements) (in [CC2022P3]), which define content requirements for the Security Target and their related assessment activities.

The risk analysis previous to the CC evaluation, that leads to the security problem definition is outside of the CC evaluation, as indicated in B.5.1 of [CEM2022]:

The PP/ST author considers the threat profile developed during a risk assessment (outside the scope of the CC, but used as an input into the development of the PP/ST in terms of the Security Problem Definition…

CRA does not mandate a specific methodology for the manufacturer's risk assessment in the legal text, while further clarifications might be provided in the future. The risk assessment associated to the CC security problem definition can be considered formally a simplified risk assessment process as it does not cover concepts such as impact, probability, or risk acceptance. Moreover, the introduction to the [CC2022P2] can be considered, as it states as follows: "*Security functional components allow for the expression of SFRs intended to counter threats in the assumed operating environment of the TOE"*. Thus, while EUCC doesn't validate or address the risk and threat assessments directly, it does so indirectly when validating the SFRs as sufficient for the applicable scenario defined by the manufacturer.

Furthermore, if the following CEM2022 guidance related to the selection of attack potential is applied, then these concepts are considered.

From [CEM2022] page 464, it can be extracted that PP/ST authors have to calculate the assumed attack potential for all different scenarios that must not violate the SFRs, then select the highest value and select a resistance for the TOE that is at least equal to this highest value:

If a PP/ST author wants to use the attack potential table for the determination of the level of attack the TOE should withstand (selection of Vulnerability analysis (AVA_VAN) component), they should proceed as follows: For all different attack scenarios (i.e. for all different types of attacker and/or different types of attack the author has in mind) which must not violate the SFRs, several passes through Table B.2 should be made to determine the different values of attack potential assumed for each such unsuccessful attack scenario. The PP/ST author then chooses the highest value resulting from this analysis in order to determine the level of the TOE resistance to be claimed from Table B.3: the TOE resistance must be at least equal to this highest value determined. For example, the highest value of attack potentials of all attack scenarios, which must not undermine the TOE security policy, determined in such a way is Moderate; hence, the TOE resistance shall be at least Moderate (i.e. Moderate or High); therefore, the PP/ST author can choose either AVA_VAN.4 (for Moderate) or AVA_VAN.5 (for High) as the appropriate assurance component.

Such an analysis is equivalent to conducting a simplified risk assessment that categorizes the risks linked to threat/attack scenarios that fall within the attack potential as non-tolerable (risks that must be addressed) and those above it as tolerable (risk is accepted). For this analysis, the factors involved in attack potential calculation given in the CC methodology are considered and would require the PP/ST authors to consider how a risk would impact the product and the likelihood of it being materialized. Therefore, when a PP/ST author conducts a vulnerability assessment based on CEM2022, the security problem definition includes implicitly the concepts of impact, probability, and risk acceptance in the risk assessment. Then, the security problem definition can be treated as the result of a general risk assessment.

Provided that the CRA will allow for such approaches, the CC risk assessment could be considered as similar to the CRA risk assessment obligation, and in any case a good starting point. Future possible additional clarification on the implementation of the risk assessment obligation under the CRA could inform also possible adaptations to the security problem definition in the CC where necessary.

On the other hand, the scope of the activities deriving from the risk analysis is not limited only to the selection of the TOE SFRs, as the CRA also mentions that other aspects related to planning, design, development, production, delivery and maintenance phases of the product shall be derived from the risk assessment. These activities are not covered by SFRs, but they can be covered by SARs in CC, e.g., ALC_DEL (TOE delivery) or ALC_FLR (Flaw Remediation Procedures). Although there is no explicit mandatory requirement in CC to derive SARs in the evaluation from a risk analysis, [CC2022P3] does include the ASE_REQ (Security requirements) assurance family, requiring that the ST author provides a rationale of why the SARs of the evaluations were chosen. In addition, ASE_REQ.1.11C subcomponent indicates that "*The statement of security requirements shall be internally consistent"* giving the following example: *"An example of an obvious inconsistency between the SARs and the remainder of the ST would be to have threat agents that are very capable, but an AVA_VAN SAR that does not protect against these threat agents.".*

For illustrative purposes an example of the security problem definition is depicted in the figure below.

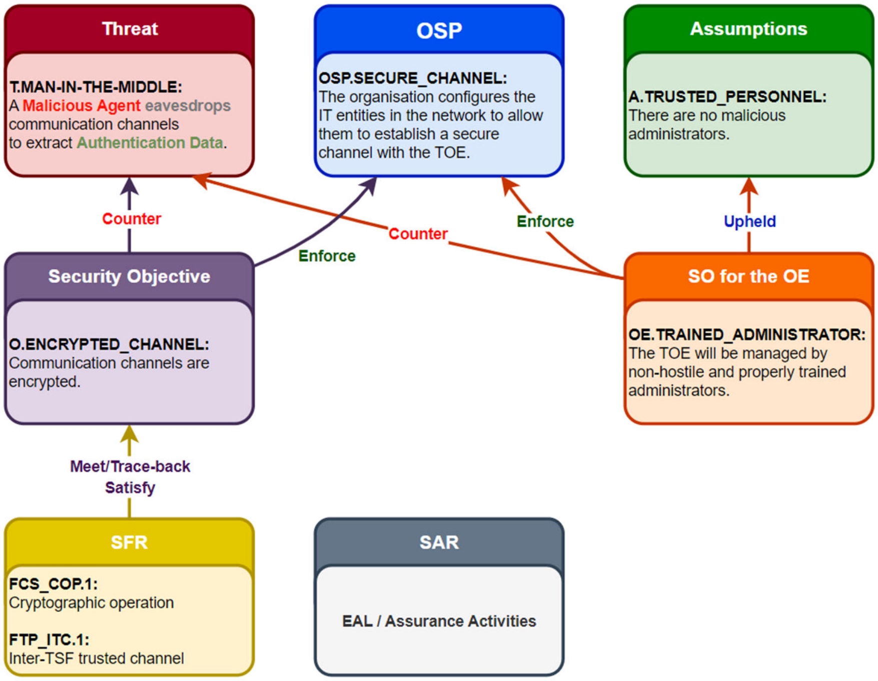

Threat
T.MAN-IN-THE-MIDDLE:
A Malicious Agent eavesdrops communication channels to extract Authentication Data.
OSP
OSP.SECURE_CHANNEL:
The organisation configures the IT entities in the network to allow them to establish a secure channel with the TOE.
Assumptions
A.TRUSTED_PERSONNEL:
There are no malicious administrators.
Counter
Counter
Enforce
Enforce
Upheld
Security Objective
O.ENCRYPTED_CHANNEL:
Communication channels are encrypted.
SO for the OE
OE.TRAINED_ADMINISTRATOR:
The TOE will be managed by non-hostile and properly trained administrators.
Meet/Trace-back
Satisfy
SFR
FCS_COP.1:
Cryptographic operation
FTP_ITC.1:
Inter-TSF trusted channel
SAR
EAL / Assurance Activities

Figure 15 Example of a Security Problem Definition in CC and its relation to the SFRs in the ST

The result of the analysis so far can be summarized as follows:

- The SFRs/SARs included in a CC ST or PP are those resulting from the Security Problem Definition, i.e., as defining the security features that the TOE shall implement in order to mitigate threats identified in the SPD. This approach is similar to the process followed in CRA, where the manufacturer's risk assessment in CRA results in the selection of those ESRs from Annex I Part I that are applicable to the product with digital elements.
- An equivalence mapping can be established between CRA ESRs and CC SFRs and SARs (i.e., when they describe equivalent same security features).
- The Security Problem Definition in CC, together with the analysis performed to select the attack potential, can be considered formally as a simplified risk assessment process, which covers the requirements of the CRA as stated in Article 13 and in Annex I, Part I (1) and (2).

Article 13 (3) also includes two further requirements regarding the cybersecurity risk assessment:

- **Taking into account the length of time the product is expected to be in use.** In the CC SPD this factor is generally considered. For example, in certain product types such as smartcards, it is foreseen that the cryptographic keys involved in critical security operations are not used more than a number of times and, after that, the chip should be killed to avoid their possible compromise. It is also implicitly taken into account through selection of the EAL depending on various factors, with higher EALs being more prone to consider the length of this period. Considering this factor in the SPD depends on the author of the ST/PP when doing the threat modelling, however during CC evaluations the ITSEF shall assess the consistency of the SFRs and SARs with the elements of the SPD and raise any inconsistencies, e.g., if the level of threat for a product in its intended use/environment is not consistent with the overall assurance level provided by the SARs chosen for the evaluation.

- **Updating the risk assessment during the support period** (in accordance with Article 13, paragraph 8). EUCC certifications will have a validity time of 5 years and at the end of that period a renewal certification needs to be carried out. If a vulnerability is found before 5 years from the certification date, then the certificate can be revoked and the product would need to undergo certification again. The certification process associated to the renewal of the certification would require a Vulnerability Analysis Report, including a risk assessment, therefore a reassessment of the Security Problem Definition, as well as an assessment of any possible new or updated security measures that the TOE could incorporate in order to be kept resistant to threats and state-of-the-art attacks in the security landscape at the moment of certification. In this sense, EUCC CABs will have a surveillance obligation of the threat landscape of the products they certify.

Therefore, CC SPD can also provide coverage for the above parts of Article 13 (3) of CRA.

Finally, CRA Article 13 (4) requires that "*Where certain essential requirements are not applicable to the product with digital elements, the manufacturer shall include a clear justification to that effect in that technical documentation*". The SPD in CC doesn't require an explicit justification of why certain SFRs/SARs in the CC aren't applicable for a particular scenario. It is rather oriented to present only those requirements that are necessary to counter the threats identified and deemed as applicable to the TOE in its intended environment. However, it should be feasible to justify on the basis of the SPD that no other SFRs or SARs are necessary for a particular scenario. As a way to draw a clear link with what is stated in CRA Article 13 (4), this study proposes that manufacturers elaborate **supplementary documentation** justifying why some ESRs in Annex I, part 1 aren't applicable for the product with digital elements on the basis of the SPD of a particular TOE in the CC evaluation. This information can be provided in the fields of the template proposed in the Annex to this study, section **"Annex III. Template: CRA conformance claims for EUCC certified products".**

This process could benefit from the future development of frameworks or guidelines that provide further guidance on how to elaborate the justifications for applicability of ESRs based on the manufacturer's risk assessment.

5.4. Scope of the assessment in EUCC vs CRA

As outlined in section **4.1 Target of Evaluation (TOE)** of this document, in EUCC evaluations the scope of assessment will be determined by the TOE (Target of Evaluation), which is the part of the system or product that falls under the scope of the EUCC evaluation. Manufacturers place on the market solutions or products certified under EUCC, but the scope of the EUCC certification (the TOE boundary) is often smaller than those products or solution, e.g., only one subsystem in a distributed architecture, or subsets of a full product.

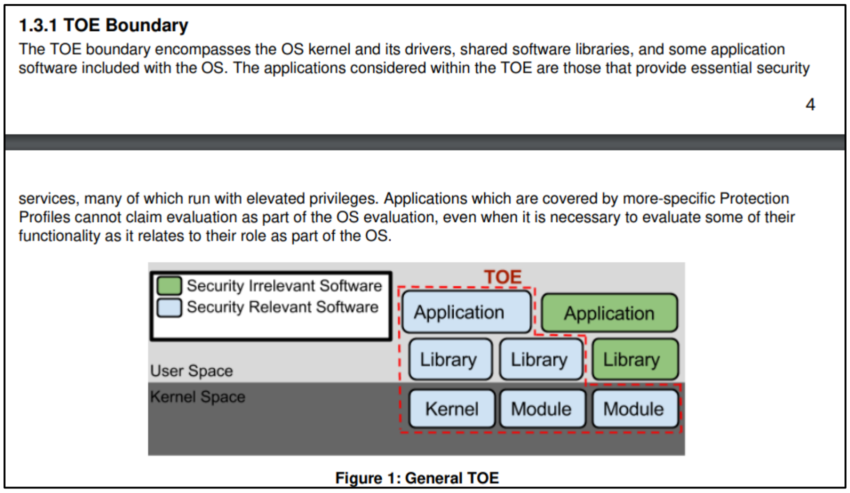
The intention behind limiting the TOE scope to something smaller than the whole product is usually to cover in the EUCC assessment only those parts of the solution that implement the SFRs under evaluation, focusing the effort of the evaluation on them. On the other hand, EUCC evaluations will be thorough and intensive, products under evaluation do not only need to meet security functional requirements, but need to be also resistant to attacks trying to bypass or tamper them and, in general, evaluation campaigns are complex, lengthy and costly, requiring an important investment on the manufacturer's end. As some parts of the products aren't security oriented or don't implement security relevant functionalities, then the investment of hardening them and having them undergoing security assessment is not always justified.

In a simplified manner, it can be assumed that the EUCC TOE boundary is set in line with the elements of the Security Problem Definition (assets to protect, threats, environment) in a way that it is ensured that those parts of the product involved in the implementation of the security solution addressing the SPD fall under the scope of the evaluation. Other parts of the products that don't fall under the TOE scope are considered security irrelevant for what it is established by the SPD.

Some examples in which the EUCC TOE scope is distinct (smaller) than the product with digital elements are as follows:

- The product is an operating system, but the TOE boundary is only the kernel, drivers and security libraries of the operating system.
- The product is a software solution, but the TOE boundary is only a library of subset of libraries in the solution.
- The product is a hardware appliance, but the TOE scope is limited to the firmware or software operating the hardware.
- The product is a mobile or IoT chipset, but the TOE scope is limited to a secure element or cryptographic module in the chipset.

As a visually illustrative example, below it is shown the boundary of the TOE defined for operating systems in the NIAP protection profile for general purpose operating systems [PP_OS]. As can be seen in the figure, the scope encompasses only the kernel, its drivers and only those software and libraries that are security-relevant, but excluding those that aren't involved in security.



1.3.1 TOE Boundary

The TOE boundary encompasses the OS kernel and its drivers, shared software libraries, and some application software included with the OS. The applications considered within the TOE are those that provide essential security

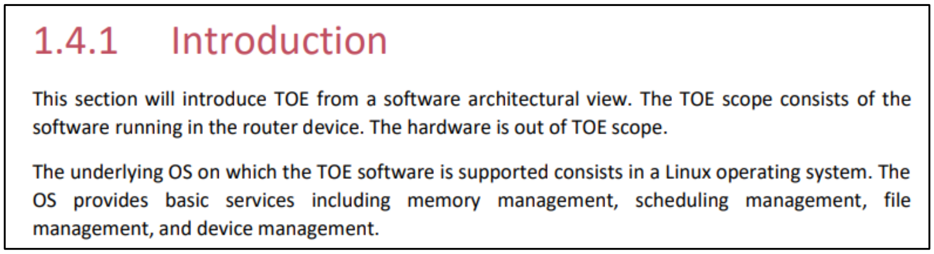
4

services, many of which run with elevated privileges. Applications which are covered by more-specific Protection Profiles cannot claim evaluation as part of the OS evaluation, even when it is necessary to evaluate some of their functionality as it relates to their role as part of the OS.

Figure 1: General TOE

Figure 16 Example of TOE boundary taken from [PP_OS]

Another visually demonstrative example is presented below, taken from the Security Target of the *Huawei NetEngine 8000&NE9000 Series Routers' Software* [NE8000_ST], which is the case of a network appliance where the certification scope is limited to the software running on the router, but not to the physical appliance on which it runs:



1.4.1 Introduction

This section will introduce TOE from a software architectural view. The TOE scope consists of the software running in the router device. The hardware is out of TOE scope.

The underlying OS on which the TOE software is supported consists in a Linux operating system. The OS provides basic services including memory management, scheduling management, file management, and device management.

Figure 17 Example of TOE boundary in [NE8000_ST]

On the other hand, the requirements established through the text of the CRA refer in all cases to the “product with digital elements” along with their “remote data processing solutions”, as in the general disposition (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.*”

The interpretation given in this report with regards to this this topic is that the requirements of CRA apply to the whole product with digital elements or, in other words, the whole product entity that is placed on the market by the manufacturer. These requirements include, among others, essential security requirements in CRA Annex I, Risk assessment related to CRA Article 13, or the scope of what needs to be covered by the user information and technical documentation requirements set out in Annexes II and VII respectively.

Based on the aforementioned considerations, it is conceivable to identify **two primary cases** concerning the alignment scenarios between the EUCC TOE scope and the scope of products with digital elements under the CRA:

a) The scope of the TOE in the EUCC evaluation includes the whole product, in other words, it is equal to the scope of the product with digital elements.
b) The scope of the TOE in the EUCC evaluation is smaller than the whole product and, therefore, smaller than the scope of the product with digital elements.

In addition, CRA essential requirements are also applicable to, and must be met by the ***remote data processing solutions*** that are part of the relevant product with digital elements which is placed on the market by the manufacturer. The concept of remote data processing is set out in the CRA as follows in Article 3(2): *‘remote data processing’ means data processing at a distance the software for which is designed and developed by the manufacturer, or under the responsibility of the manufacturer, and the absence of which would prevent the product with digital elements from performing one of its functions;*

Moreover, CRA recital 11 defines the main aim of data processing: *“ensures that such products are adequately secured in their entirety by their manufacturers, irrespective of whether data is processed or stored locally on the user’s device or remotely by the manufacturer.”*. This recital also establishes it scope as *“processing or storage at a distance falls within the scope of this Regulation only in so far as it is necessary for a product with digital elements to perform its functions.” “Cloud solutions constitute remote data processing solutions within the meaning of this Regulation only if they meet the definition laid down in this Regulation.”*

Examples of these type of elements, provided also in CRA recital 11 are: *“Such processing or storage at a distance includes the situation where a mobile application requires access to an application programming interface or to a database provided by means of a service developed by the manufacturer. In such a case, the service falls within the scope of this Regulation as a remote data processing solution.” “For example, cloud enabled functionalities provided by a manufacturer of smart* *home devices that enable users to control the device at a distance fall within the scope of this Regulation."*

Moreover, exclusions from scope are also set out in recital 11 as follows: *"The requirements concerning the remote data processing solutions falling within the scope of this Regulation do therefore not entail technical, operational or organisational measures aiming to manage the risks posed to the security of a manufacturer's network and information systems as a whole." "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."*

The interpretation taken when elaborating this study is taking into account the text of the CRA, i.e., that not all elements or systems with which the product with digital elements (deployed on-premises) communicates need to be considered as remote data processing solutions according to the definition given in CRA. It is noted that this is a concept that will be subject to further guidance by the European Commission in line with Article 26 of the CRA. The highlights of the interpretation taken in this study are:

- If the ICT product hosted remotely is needed to boot or configure the TOE, then it is considered a remote data processing solution. Examples:
    - Remote management console in the cloud without which a firewall cannot be configured.
    - Dashboard for an enterprise device management solution, deployed individually in computers of the customer's network, that is hosted and accessed on the manufacturer's cloud. Without it, the control of the IT inventory cannot be done.
- If the ICT product can be booted and configured without that remote ICT product, then it is not considered a remote data processing solution. Examples:
    - A connected TV that can be configured and used to watch TV channels connectionless. With a network protection, it would have more functionalities, but the basic ones are available with it and the TV can be booted, configured and used normally without it.
    - A Point of Interaction (payment terminal) that can be booted and functional without the server-side payment server. While it cannot be used in remote-checked parts of the operations, the terminal is functional.

As in with the product with digital elements, it is possible to envision two cases, one where the remote data processing solution is included in the scope of the EUCC evaluation, and another case where it is out of the scope and, hence, it becomes part of operational environment.

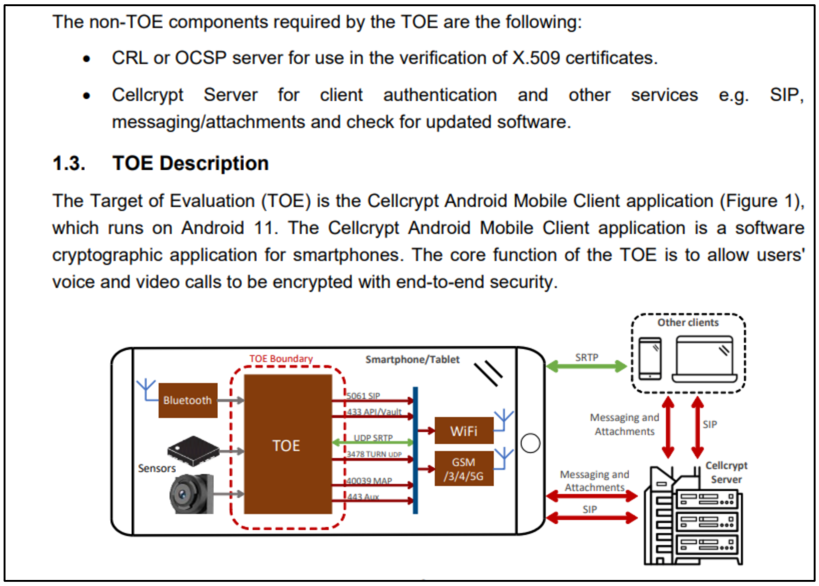
Since these remote data processing solutions can be entities hosted "in the cloud", either on the manufacturer's owned systems or in third parties hosting infrastructure. This case becomes even more difficult in the context of EUCC evaluations, as due to the CC methodology followed in these, the CABs need to be able to fully control the environment in which the TOE is installed, e.g., being able to install all subsystems of the product on the ITSEF's evaluation networks. When remote solutions can be seamlessly installed both on-premisses or in the cloud, including these solutions in-scope brings no trouble. However, if the component needs to reside natively in the cloud, then this type of environment does not provide the necessary conditions for ITSEF to conduct tests on the remote part of the product, as required by the CC methodology.

In addition, the EUCC certification paradigm restricts the coverage of certification to the exact version of the product that was evaluated by the ITSEF. If the cloud-hosted part of the certified solution were to be under the scope of the certification, any update that increases its version would cause the newer version to be different from the certified one and, therefore not covered by the certification. As solutions hosted in the cloud tend to be subject of rapid and agile update cycles, covering the on-cloud part of the product in the certification could result also impractical under this scenario.

It is actually quite common in the CC certification industry to exclude from the certification scope those parts of the system residing in the cloud. This situation is expected to occur in future EUCC certifications in the market as well. Some examples are:

- **Endpoint Detection and Response** software that rely on an update server or **management console,** which is also in charge of distributing updates to the threat databases. It's usual that the remote console is left out of the scope of the evaluation, and the TOE comprises only the agent installed on-premise in the customer's workstations.
- **Network devices administered from in-cloud management systems**. Those systems include the interface and the engine to establish the configuration of one or more devices in the network, and those devices are deployed in the on-premises customer's network. Commonly, the management consoles are out of the scope of the evaluation.

An example of a mobile application use for end-to-end encrypted calls that relies on a server to provide this function can be found in [CELLCRYPT_ST]. The figure below, taken from that ST, illustrates this case in which the server-side software, required to perform the encrypted calls, is not included in the scope of the evaluation and it is identified as non-TOE:



The non-TOE components required by the TOE are the following:

- CRL or OCSP server for use in the verification of X.509 certificates.
- Cellcrypt Server for client authentication and other services e.g. SIP, messaging/attachments and check for updated software.

1.3. TOE Description

The Target of Evaluation (TOE) is the Cellcrypt Android Mobile Client application (Figure 1), which runs on Android 11. The Cellcrypt Android Mobile Client application is a software cryptographic application for smartphones. The core function of the TOE is to allow users' voice and video calls to be encrypted with end-to-end security.

Figure 18 Example of TOE boundary in [CELLCRYPT_ST]

Note: there are also certain cases of products of the same type as those in the examples mentioned, where the administration console can be deployed on-premise, thereby including it within the scope of Common Criteria certification.

Consequently, the secondary factors to consider regarding the scope of the evaluation when the product with digital element includes remote data processing solutions, is not only whether they are in-scope of the TOE, but also if they can be evaluated under an on-premise deployment.

In general, any part of the product with digital element that hasn't been included in the scope of the EUCC evaluation (TOE), doesn't count with the assurance provided by the assessment activities associated conducted by the CAB according to the SARs in scope. Those activities would exclude, in these cases, all non-TOE parts (even if they are part of the same product with digital elements, or part of the remote data processing solution), that will be considered as operational environment and, as such, will be fully out of scope of existing CC assessments and future EUCC assessments.

Some main areas can be identified where a narrower scope of the TOE compared to the scope of the product with digital elements would affect the compliance of the "non-TOE but in-product" components with the CRA:

1) **Compliance with the ESRs in CRA Annex I part I**, **mainly related with SFRs in EUCC**. In fact, this impact will depend on which ESRs (then SFRs and SARs) have been included in the scope of the assessment in accordance with the manufacturer's risk assessment. Arguably, it could be said that the scope of the assessment already covers the part of the product that implements the security mechanisms in charge of protecting the relevant assets (as per the SPD), which can be true in any cases, however **certain ESRs have product-wise relevance**, and not only relevance for the security-core of the product, e.g., Annex I, Part I, (2)(c), requiring the product to be able to receive security updates. In a multi-component product, the EUCC evaluation would verify this requirement (by assessment of equivalent SFRs) only for those components under the TOE scope, but it won't be verified whether other components, e.g., client-side software, or user-interface/non-security agent, are updatable.

   Another illustrative case would be that non-TOE parts, subcomponents, or product layers in relationship with AVA_VAN vulnerability analysis. The definition of the assurance component AVA_VAN.2 in [CC2022P3] includes the following assurance element: *"AVA_VAN.2.2E*
   The evaluator shall perform a search of public domain sources to identify potential vulnerabilities in the TOE the components in the list of third party components, ***AVA_VAN.2.2E***
   The evaluator shall perform a search of public domain sources to identify potential vulnerabilities in the TOE, ***the components in the list of third party components, and specific IT products in the environment that the TOE depends on.***" When AVA_VAN.2 or higher is included in the scope of the evaluation, the evaluator's vulnerability analysis will cover non-TOE parts that are part of the product, and even of other IT products. However, this assurance element doesn't exist in AVA_VAN.1, then when this SAR is the highest AVA_VAN component included in the evaluation, the non-TOE parts of the product won't be subject of vulnerability assessment during the evaluation. However, in some cases the SPD will assume that these parts are considered as trusted. Therefore, when the claimed AVA_VAN level in the EUCC certification is lower than AVA_VAN.2, it won't be always possible to provide any guarantee that the non-TOE parts of the product are free of known exploitable vulnerabilities.

2) **Compliance with the ESRs in Annex I part II of CRA, mainly related with SARs in EUCC**. The requirements in this group apply mainly to vulnerability management and, again, the EUCC certification wouldn't ensure that they are complied with for non-TOE parts that are in-scope of the product with digital elements. It could be the case that the vulnerability management policies or updating mechanisms wouldn't apply to parts of the solution, or that the SBOM is not provided for the full scope of the product, among others.

3) **Risk assessment required by CRA**, as a TOE scope narrower than the CRA scope would allow not considering risks or threats to assets confined within the boundary of the parts of the product that aren't considered within the EUCC TOE scope. This links indirectly with 1) and 2), as this lack of risk assessment in those parts would prevent designing the relevant security mechanisms (ultimately as SFRs and CRA ESRs) that should aim to protect the aforementioned assets.

At the end, this scenario can be summarized as that where the scope of the TOE in an EUCC certification could be narrower than that of the CRA product with digital elements (because the TOE doesn't include part of the product, because the remote data processing element is not in TOE scope, or both). In this situation, the EUCC certification would ensure that the CRA ESRs are met for those parts of the product that fall under the scope of the evaluation (whereas depending on but, in principle, not for those that do not, i.e., refer to section **7.4 Remote data processing solutions** for a detailed analysis on the challenges related to this subject that might arise for remote data processing solutions when they cannot be included in the scope of the EUCC assessment, although preferably they should be included if possible, with relevant SFRs and SARs).

Later chapters of this study explore on the options or way forwards that could be designed in order to address this situation. One of them could be using the EUCC certificate to demonstrate compliance with the CRA ESRs only for those subcomponents of the product covered by the EUCC certification, but using other mechanisms different from those in a EUCC evaluation in order to prove that compliance for the remaining parts of the product.

5.5. EUCC support for User Information and Technical Documentation

CRA sets out not only a number of essential security requirements, those in Annex I, but also establishes requirements on manufacturer's applying to the information that they need to provide to users of their products, and for the technical documentation to be provided to CABs. In addition to the ESRs in Annex I, the CRA also sets out obligations for the manufacturer with respect to Technical Documentation (in CRA Annex VII CONTENTS OF THE TECHNICAL DOCUMENTATION) and User Instructions related documentation (in CRA Annex II, INFORMATION AND INSTRUCTIONS TO THE USER).   The overall view of these categories is illustrated in the image below.

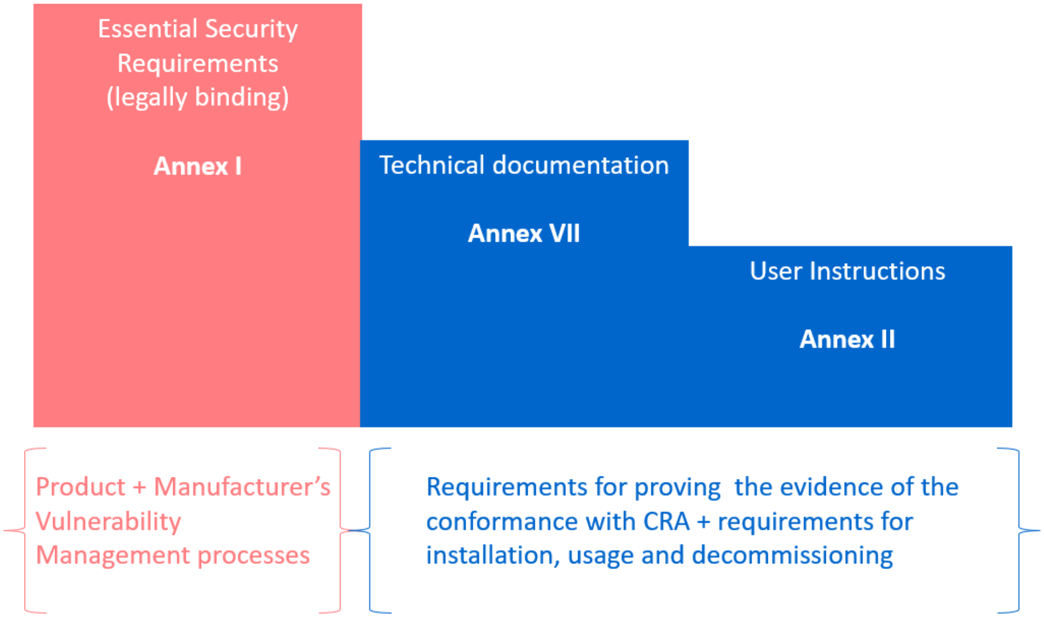

Essential Security Requirements (legally binding)
Annex I
Technical documentation
Annex VII
User Instructions
Annex II
Product + Manufacturer's Vulnerability Management processes
Requirements for proving the evidence of the conformance with CRA + requirements for installation, usage and decommissioning

Figure 19 Classification of requirements by CRA Annex

As outlined in previous sections of this chapter, the CC standard that will be used in EUCC scheme provides two types of technical elements for fulfilling CRA ESRs: SFRs and SARs. CC SFRs describe security functionality implemented by the product and that is in the scope of the evaluation., Therefore they do not address CRA requirements targeting manufacturer's processes. However, many of the SAR families in CC are specifically intended for this purpose. As already mentioned, some of them focus on the assessment of manufacturer's procedures related to the product lifecycle, or they relate to the guidance provided to users of EUCC-certified products.

In this context, although the requirements for manufacturers outlined in CRA Annexes II and VII could be addressed outside of the EUCC certification, certain technical elements within the EUCC do overlap with these requirements. Consequently, it may be advantageous for manufacturers to leverage the efforts used in generating the evidence used during a EUCC evaluation in order to meet the CRA requirements in those annexes.

Some of the requirements in CRA Annexes II and VII are, however, not security-relevant or not security-oriented and therefore it's not feasible to address them through technical elements of the CC.

The two tables below summarize which SARs could address requirements in CRA Annex II and CRA Annex VII, where they are security-relevant, but the detailed analysis that results in this selection can be found in Annex **"ANNEX I. Mapping the CRA Requirements for EUCC certification process (detailed analysis)"** In some cases, if [CC2022P3] doesn't contain a suitable SAR for a specific CRA requirement, an Extended SAR is proposed (which is a SAR that needs to be newly created), marked with the keyword **extended.**

CRA Annex II requirement	**SARs in EUCC/CC**	**Notes**
At minimum, the product with digital elements shall be accompanied by:	-	-
1. *the name, registered trade name or registered trademark of the manufacturer, and the postal address, the email address or other digital contact as well as, where available, the website at which the manufacturer can be contacted;*	N/A: Not security-relevant	Information to be included in the ST, i.e., in an annex with specific CRA information, but not under the scope of the EUCC evaluation.
2. *the single point of contact where information about vulnerabilities of the product with digital elements can be reported and received, and where the manufacturer's policy on coordinated vulnerability disclosure can be found;*	ALC_FLR.2 Flaw reporting procedures	The point of contact for vulnerability reporting is included in the flaw remediation guidance for users required by ALC_FLR.2. Also covered in EUCC Article 33.2 "2. The holder of an EUCC certificate shall maintain and publish appropriate methods for receiving information on vulnerabilities related to their products from external sources, including users, certification bodies and security researchers."
3. *name and type and any additional information enabling the unique identification of the product with digital elements;*	ASE_INT.1 ST Introduction AGD_PRE.1 Preparative Procedures	This information is publicly available in the EUCC Security Target (ASE) and available to customers in the AGD_PRE user guidance.
4. *the intended purpose of the product with digital elements, including the security environment provided by the manufacturer, as well as the product's essential functionalities and information about the security properties;*	ASE_INT.1 ST Introduction ASE_SPD.1 Security problem definition ASE_OBJ.1 Security objectives for the operational environment ASE_REQ.1 Direct rationale security requirements AGD_PRE.1 Preparative Procedures AGD_OPE.1 Operational user guidance	This information is publicly available in the EUCC Security Target (ASE) and available to customers in the AGD_PRE and AGD_OPE user guidance.

5. *any known or foreseeable circumstance, related to the use of the product with digital elements in accordance with its intended purpose or under conditions of reasonably foreseeable misuse, which may lead to significant cybersecurity risks;*	AGD_OPE.1 Operational user guidance	This information is included in the TOE user guidance required by AGD_OPE.1
6. *where applicable, the internet address at which the EU declaration of conformity can be accessed;*	N/A: Not security-relevant	Information to be included in the ST, i.e., in an annex with specific CRA information, but not under the scope of the EUCC evaluation, as there will be an EUCC Certified Solution the Certificate will be published at ENISA Website.
7. *the type of technical security support offered by the manufacturer and the end-date of the support period during which users can expect vulnerabilities to be handled and to receive security updates;*	SARs implementing the (technical) patch mechanism involved in EUCC's patch management procedure – this study recommends to instantiate it through the technical elements defined in [ISO_TS_9569]	
8. *detailed instructions or an internet address referring to such detailed instructions and information on:*	-	-
(a) the necessary measures during initial commissioning and throughout the lifetime of the product with digital elements to ensure its secure use;	AGD_PRE.1 Preparative Procedures AGD_OPE.1 Operational user guidance	
(b) how changes to the product with digital elements can affect the security of data;	AGD_OPE.1 Operational user guidance SARs implementing the (technical) patch mechanism involved in EUCC's patch management procedure – this study recommends to instantiate it through the	

	technical elements defined in [ISO_TS_9569]	
(c) how security-relevant updates can be installed;	SARs implementing the (technical) patch mechanism involved in EUCC's patch management procedure – this study recommends to instantiate it through the technical elements defined in [ISO_TS_9569]	
(d) the secure decommissioning of the product with digital elements, including information on how user data can be securely removed;	AGD_DEC.1 Decommissioning procedures (Extended)	
(e) how the default setting enabling the automatic installation of security updates, as required by Annex I, Part I, point (c), can be turned off;	AGD_OPE.1 Operational user guidance	AGD_OPE.1 shall provide information on how to use the interface to the TOE Security Functionality, one of them being the enabling/disabling of automatic updates, according to the patch mechanism chosen to comply with ESR 2(c) in CRA Annex I, part 1.
(f) where the product with digital elements is intended for integration into other products with digital elements, the information necessary for the integrator to comply with the essential requirements set out in Annex I and the documentation requirements set out in Annex VII.	Implicit. See comments.	In EUCC evaluations, part of the documentation required as per equivalence with that in Annex VII will not be distributed to 3rd party vendors, not even to integrators in composition processes, e.g. the proprietary design documentation about the product internals or details about the lifecycle of the product. However, this study proposes to comply with this requirement by setting out parts of the technical documentation associated to the SARs mapped to requirements in Annex VII that belong to the evaluation information that is

		public or that is part of the documentation delivered to the integrator. The set of documentation of the EUCC evaluation that is delivered to integrators consists of: ▪ The Security Target (ASE). ▪ The user guidance (AGD). As such, the documentation belonging to the scope of other assurance classes is not delivered to third parties (other than CABs). To address this gap, the following solutions are proposed for the requirements of Annex VII that pose a conflict with the above diffusion policy: ▪ Requirement 1 (d): “*where the product with digital elements is a hardware product, **photographs or illustrations showing external features, marking and internal layout**; “* => **Way forward**: manufacturers shall include such illustrations and layout and interfaces of the products either in the Security Target or in the guidance for integrators (AGD). Internal design details (i.e., subsystem decomposition required by ADV_TDS.1) don’t need to be distributed for integration. Documentation of TOE interfaces that is relevant for integration shall be included in AGD rather than in ADV_FSP documentation.

		▪ Requirement 2 (a)**:** manufacturers shall include only high-level design details (i.e., commensurate with ADV_TDS.1 Basic design) in the Security Target or in the user guidance for integrators (AGD). Internal design details (i.e., subsystem decomposition required by ADV_TDS.1 or higher) don't need to be distributed for integration. ▪ Requirement 2(b) Policy for vulnerability handling and disclosure, as well as (where applicable) SBOM shall be distributed to integrators. Internal details of vulnerability handling process related to ALC_FLR can be kept in the non-distributable documentation scope. ▪ Requirement 2(c): same as for requirement 2(b). Moreover, the high-level information about the TOE lifecycle related to production and monitoring processes shall be included in the Security Target. ▪ Requirement 6: The reports of tests and vulnerability handling aren't items that are necessary for the purpose of technical integration. The integrator can rely on the verification of these reports that is carried out during the CAB during the EUCC evaluation, as the EUCC certification will provide assurance for that. ▪ Requirement 8: If it has been deemed as applicable to provide the SBOM with the technical documentation, the SBOM has to be distributed to the integrator.

9. *If the manufacturer decides to make available the software bill of materials to the user, information on where the software bill of materials can be accessed.*	Not directly supported by EUCC	Manufacturers can use the template in the Annex to this study, section **“Annex III. Template: CRA conformance claims for EUCC certified products”** to provide the information about the location of the SBOM.

Table 3 Coverage of CRA Annex II requirements

CRA Annex VII requirement	**SARs in EUCC/CC**	**Notes**
The technical documentation referred to in Article 31 shall contain at least the following information, as applicable to the relevant product with digital elements:		
1. *a general description of the product with digital elements, including:*	-	-
(a) *its intended purpose;* ***(b)*** *versions of software affecting compliance with essential requirements;* ***(c)*** *where the product with digital elements is a hardware product, photographs or illustrations showing external features, marking and internal layout;* ***(d)*** *user information and instructions as set out in Annex II;*	ASE_INT.1 ST Introduction ASE_TSS.1 TOE summary specification	
2. *a description of the design, development and production of the product with digital elements and vulnerability handling processes, including:*	-	-
(a) *necessary information on the design and development of the product with digital elements, including, where applicable, drawings and schemes and a description of the system architecture explaining how software components build on or feed into each other and integrate into the overall processing;*	ADV_TDS.1 Basic design	
(b) *necessary information and specifications of the vulnerability handling processes put in place by the manufacturer, including the software bill of materials, the coordinated vulnerability disclosure policy, evidence of the provision of a contact address for the reporting of the vulnerabilities and a description of the technical solutions chosen for the secure distribution of updates;*	ALC_FLR.2 Flaw reporting procedures SARs implementing the (technical) patch mechanism involved in EUCC’s patch management procedure – this study recommends to instantiate it through the	-

	technical elements defined in [ISO_TS_9569] ALC_SBM.1 Software bill of materials (Extended)	
(c) *necessary information and specifications of the production and monitoring processes of the product with digital elements and the validation of those processes;*	ALC_LCD.1 ALC_FLR.2 Flaw reporting procedures SARs implementing the (technical) patch mechanism involved in EUCC's patch management procedure – this study recommends to instantiate it through the technical elements defined in [ISO_TS_9569]	
3*. an assessment of the cybersecurity risks against which the product with digital elements is designed, developed, produced, delivered and maintained as laid down in Article 13 of this Regulation, including how the essential requirements set out in Annex I, Part I, are applicable;*	ASE_SPD.1 Security problem definition ASE_OBJ.2 Security objectives ASE_REQ.1 Direct rationale security requirements	Manufacturers shall also indicate in the template in the Annex to this study, section **"Annex III. Template: CRA conformance claims for EUCC certified products"** the ESRs that aren't applicable for the product with digital elements.
4. *relevant information that was taken into account to determine the support period as referred to in Article 13(8) of the product with digital elements;*	Not directly supported by EUCC, but implicitly they take into consideration the 5 years validity of the EUCC certificate.	Manufacturers should also indicate in the template in the Annex to this study, section **"Annex III. Template: CRA conformance claims for EUCC certified products"** which elements of the SPD in the ST were taken into account in relationship with the duration of the support period.
5. *a list of the harmonised standards applied in full or in part the references of which have been published in the Official Journal of the European Union, common specifications as set out in Article 27 of this Regulation or European*	N/A: Not relevant to security	

cybersecurity certification schemes adopted pursuant to Regulation (EU) 2019/881 pursuant to Article 27(8) of this Regulation, and, where those harmonised standards, common specifications or European cybersecurity certification schemes have not been applied, descriptions of the solutions adopted to meet the essential requirements set out in of Annex I, Parts I and II, including a list of other relevant technical specifications applied. In the event of partly applied harmonised standards, common specifications or European cybersecurity certification schemes, the technical documentation shall specify the parts which have been applied;		
6. *reports of the tests carried out to verify the conformity of the product with digital elements and of the vulnerability handling processes with the applicable essential requirements as set out in Annex I, Parts I and II;*	ATE_FUN.1 Functional testing ATE_DPT.1 Testing: basic design Periodic Security Review and Testing of the TOE (ALC_PSR.1) - Extended	
7. *a copy of the EU declaration of conformity;*	N/A: Not relevant to security	
8. *where applicable, the software bill of materials, further to a reasoned request from a market surveillance authority provided that it is necessary in order for this authority to be able to check compliance with the essential requirements set out in Annex I.*	ALC_SBM.1 Software bill of materials (Extended)	

Table 4 Coverage of Annex VII requirements

6. Analysis of the EUCC certification landscape for Critical and Important products

Editor's note: at the date of release of this report, there were no EUCC certified products in the market as the Implementing Act had been released on January 2024 and the industry is still adapting (i.e., through ongoing accreditation of CABs and adaptations in national schemes). The description of the landscape provided in this section is based on the Common Criteria certifications existing in the industry, which are expected to be replaced in the EU by EUCC certifications after the EUCC transition period. Consequently, this section often refers to CC rather than to EUCC when describing the status of the industry or the existing certifications in it.

This chapter aims to provide a general vision of the EUCC certification landscape and analyses the situation of the mainstream categories of products certified on the market. The final objective is to measure to which extent CC-certified products that currently exist in the industry meet the CRA ESRs through the CC technical elements included in their CC certificates, in accordance with the technical factors of compliance that have been developed so far in this study.

The analysis here performed is based in both the categories of Critical and Important products (class I and II) in the CRA as a representative sample of products that could choose a European cybersecurity certification scheme (a.k.a. EUCC) as method to demonstrate conformity with CRA, according to Article 32 of the legislation.

As the categories of products falling into the list of important products with digital elements in CRA Annex III and the critical ones in Annex IV are numerous, this study won't perform an in-depth detailed assessment for each individual product category. Instead of that, a general summarized assessment will be done for every category of product and the specific analysis will be carried out for a representative sample of categories.

Disclaimer: Please note that this document provides guidance based on the current understanding of the CRA categories of Critical and Important products, from an EUCC perspective, on the time this report has been published.

It must be noted as well that other products with digital element that don't fall into any of the categories of important products of CRA Annex III or critical products in CRA Annex IV exist on the market. These don't require the demonstration of conformity with CRA through a third-party assessment. For those type of products, it is possible to perform a self-assessment according to the internal control procedure (based on module A) set out in CRA Annex VIII, as established in Article 32 of CRA. Those types of products haven't been included in the scope of the analysis performed in this study. However, the products in this group that obtain an EUCC certification could potentially benefit from the ways to meet CRA through EUCC that this study explores.

6.1. Use of protection profiles in the certification industry

In order to perform a correct lecture of the industry situation when designing solutions for integrating the EUCC technical elements required for CRA compliance, it is essential to analyse how the CC industry behaves. During the ICCC 2023 (International Common Criteria Conference) held in Washington DC, the cybersecurity company jtsec Beyond IT Security presented the results of their CC Technical support for the preparations of the implementation of the CRA: Deliverable A data gathering tool and presented relevant statistics for the CC certification industry. Those statistics are obtained by gathering the data about CC certificates that are published in both https://commoncriteriaportal.org and in the websites of the NCCAs.

One of the most significative statistics presented was the use of protection profiles during the year 2023 (up to 30th of September) that is presented below:

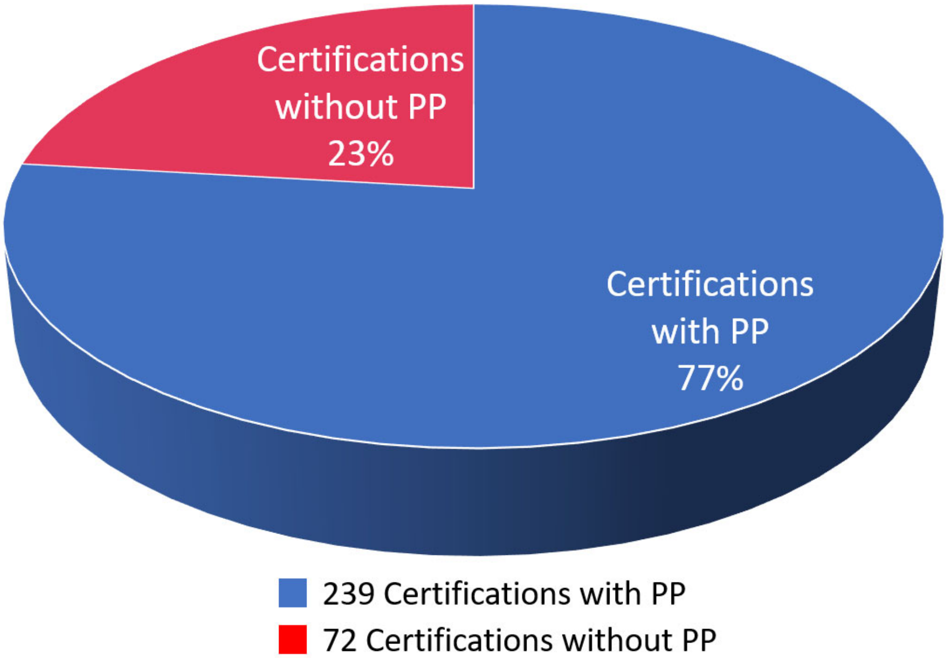


Figure 20 Percentage of use of PPs in CC certifications between January and October 2023

The chart shows that 77% of the certifications carried out during 2023 were compliant with a Protection Profile. The numbers for the previous year are quite similar, for example, **in 2022 75% of the CC certifications were compliant with a protection profile**, according to the report published in **2022:** In https://www.jtsec.es/files/2022%20CC%20Statistics%20Report.pdf.

This trend clearly indicates that the CC certification industry is primarily driven by the use of protection profiles. These profiles have been meticulously developed over the years by specialized companies, technical working groups, SDOs, and NCCAs, all aiming to consolidate and streamline the certification strategies for vendors of similar products. The ongoing evolution and refinement of these protection profiles reflect the collective expertise and concerted efforts within the industry.

Given this context, it becomes evident that the predominant practice in the CC certification industry involves the application of these protection profiles. This reality cannot be overlooked when conducting any comprehensive analysis of the industry. Ignoring this crucial factor would result in an incomplete and unrealistic assessment. Consequently, any proposed options for this study must thoroughly consider the role and influence of protection profiles to ensure a relevant and accurate evaluation.

Moreover, jtsec Beyond IT Security provided ENISA with the results from their statistical generation tool, which identified the ten most commonly used protection profiles during the five-year period from 2019 to 2023. In the image below the following code colour is used:

a) A red square surrounds protection profiles that are used in certifications of types products that typically fit categories of critical products under CRA Annex IV.

b) A green square surrounds protection profiles that, **in certain scenarios,** are used to certify types of products that, **in certain industry cases,** could fit categories of important products under CRA Annex III.

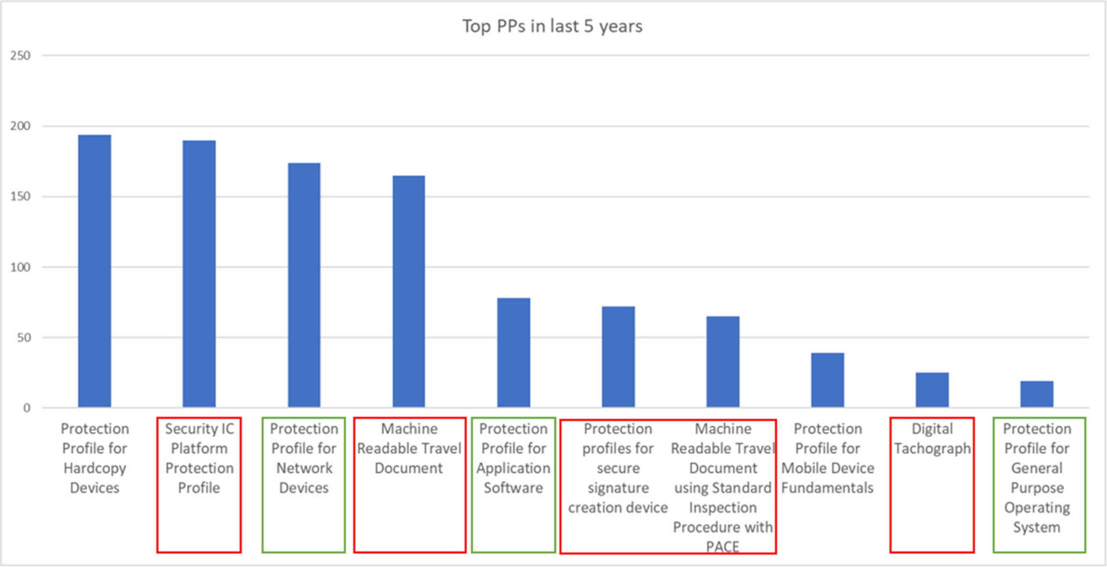


Figure 21 Top used PPs between 2019 and 2023

The protection profiles in the chart are used for the following types of technologies described in the below table:

Protection profile	Number of product certified with the PP (last 5 years)	Type of product	Type of Important or Critical Product in CRA
Protection Profile for Hardcopy Devices	194	Multi-function devices such as printers/scanners/faxes.	N/A
Security IC Platform Protection Profile	190	Smartcards and similar devices	Annex IV, 3. Smartcards or similar devices, including secure elements.
Protection Profile for Network Devices	174	Network appliances such as routers, firewalls, switches, etc.	
Machine Readable Travel Documents	165	Electronic passport	Annex IV, 3. Smartcards or similar devices, including secure elements.
Protection Profile for Application Software	78	General or specific-purpose software	Applicable to several categories of software in Annex III

Protection profiles for secure signature creation devices	72	Hardware Security Modules	Annex IV, 1. Hardware Devices with Security Boxes;
Machine Readable Travel Document using Standard Inspection Procedure with PACE	65	Electronic passport	Annex IV, 3. Smartcards or similar devices, including secure elements.
Protection Profile for Mobile Device Fundamentals	39	Mobile Devices for use in an enterprise.	N/A
Digital Tachograph	25	Tachographs in vehicle systems	Annex IV, 1. Hardware Devices with Security Boxes;
Protection Profile for General Purpose Operating System	19	Operating systems	Annex III, 10. Operating systems;

Table 5 Top PPs vs Technologies

The most used PP is the PP for hardcopy devices [CPP_HARDCOPY], however, there isn't a corresponding product category in CRA, as these type of devices (multi-function printer, scanners, faxes, etc.) don't fall into any of the categories of important or critical products with digital elements defined in CRA, but according to CRA Article 32(1)(d) their compliance with CRA could be potentially demonstrated through an EUCC evaluation. The chart shows that products of this type are frequently being CC certified in the market, so in the future they could potentially take advantage of EUCC certifications to comply with CRA. The most common category of CC-certified products is that of Smartcards and similar devices including security ICs, with several PPs in that list.

A similar situation can be observed for the type of device that is the Target of Evaluation in certifications that use the Protection Profile for Mobile Device Fundamentals [PP_MDF]. This PP appears as one of the most commonly used in the statistics, however, the type of TOE targeted by this PP is a mobile device (i.e., smartphones, tablets) including its whole hardware, firmware and software, which cannot be mapped specifically to any of the categories of important or critical products in CRA. However, some individual parts of this type of products, e.g., its operating system, could be related to other categories of important products.

Although they don't appear in the above list, there are two additional protection profiles worth to be mentioned. Java Card System - Open Configuration [PP_JCOS_OPEN] and Java Card System - Closed Configuration [PP_JCOS_CLOSED] are used widely in the industry for Javacard Systems as two different configurations which, If accounted together, would be in the top 10 most used PPs.

It must be acknowledged that the statistics presented regarding the use of PPs in CC certifications take into account both those carried out within and outside the EU, including with PPs certified outside the EU. Although this study acknowledges that EUCC will be applied only in the EU, all the mentioned PPs are related to products with digital elements that, when placed on the market within the EU, must comply with the CRA. An example could be the hardcopy devices themselves or many network devices (switches, routers, etc.) that are consumed within the EU although generally manufactured and CC-certified in non-EU countries with non-EU PPs.

In the subsequent sub-sections, where specific product categories will be analysed, particular emphasis will be placed on examining the protection profiles employed in the certification of products within those categories. This focused approach will provide deeper insights into how protection profiles shape certification practices and will highlight their significance in maintaining industry standards.

6.2. Critical Products with digital elements (Annex IV)

The Annex IV of CRA establishes the following categories of Critical products:

1. Hardware Devices with Security Boxes
2. Smart meter gateways within smart metering systems as defined in Article 2(23) of Directive (EU) 2019/944 of the European Parliament and of the Council
   i. and other devices for advanced security purposes, including for secure cryptoprocessing
3. Smartcards or similar devices, including secure elements.

Given their relevance and that they pose one of the highest degrees of criticality in the certification industry, each of the critical product types will be treated separately.

6.2.1. Hardware Devices with Security Boxes

Hardware devices with security boxes are certified in the CC industry following the supporting documentation and instructions developed by SOGIS (https://www.sogis.eu/) for the technical domain that is named as well *Hardware Devices with Security Boxes.* [EUCC] includes this technical domain as one of those which can be used for certification at levels AVA_VAN.4 and AVA_VAN.5. These are products composed of various discrete components mounted on one or more printed circuit boards. A substantial part of the necessary security functions relies on a hardware physical envelope, known as a "Security Box", which includes countermeasures against direct physical attacks. Examples of such products include payment terminals, tachograph vehicle units, taxi meters, access control terminals, and Hardware Security Modules.

Protection Profiles

With respect to certification of this type of products, SOGIS establishes in https://www.sogis.eu/uk/pp_en.html various CC **protection profiles** depending on the typology of product. These profiles are already included in [EUCC] Annex III as recommended PPs:

1. For Point Of Interaction (POI), such as payment terminals, there are various options of protection profiles defines in the SOGIS website, as base PPs with different variants depending on the logical scope, but with [PP_POI] defining all the base protection profiles.

2. For Hardware Security Modules (HSM), the following protection profiles are defined by SOGIS:
   i. Cryptographic Module for CSP Signing Operations with Backup - PP CMCSOB [PP_CMCSOB]
   ii. Cryptographic Module for CSP key generation services - PP CMCKG [PP_CMKCKG]
   iii. Cryptographic Module for CSP Signing Operations without Backup - PP CMCSO [PP_CMCSO]

3. For Digital tachographs, the following protection profiles are published by SOGIS:
   i. Digital Tachograph - Vehicle unit [PP_TACH_VU].
   ii. Digital Tachograph - External GNSS Facility (EGF PP) [PP_TACH_EFG].
   iii. Digital Tachograph - Motion Sensor (MS PP) [PP_TACH_MS].

For **all of these PPs**, the type of conformance is **strict.**

Scope of the EUCC assessment

In the case of **Point Of Interactions**, the TOE in scope of the CC certification are payment terminals with integrated circuits card based online and offline transaction capabilities, which products range from simple Pin entry device with PIN keypad, display and IC and Magnetic Stripe Card readers to complete terminals (POI) that manage transaction data and provide external communications capabilities. However, payment applications are outside the scope of the certification for the PP, although it contemplates extending within a specific product evaluation to cover payment applications within scope (outside of the PP SPD)[13].

In the case of **HSMs**, taking as a reference the [PP_CMCSOB], the scope of the certification covers a Cryptographic Module (CM) used for the creation and usage of Certificate Service Provider Signature-Creation Data (CSP-SCD), including software and hardware.

In the case of the **digital tachograph** technology type, the different parts of the tachograph are certified separately with different PPs (vehicle unit, external GNSS facility, motion sensor). In every case, the scope of the certification covers the HW and the SW (if applicable) running on the top of it.

These types of products might have been supported by remote processing elements when integrated as a part of a solution but the scope of the CC certification given by the appropriate PPs reflects the state in which manufacturers sell them, i.e. to integrators.

In the same way, remote processing elements might be needed in integrated solutions that fall in the scope of what happens in integration, after the manufacturer of the device has commercialized it. Therefore, the products described by these PPs don't include in general remote data processing elements.

As a conclusion, in general, **the scope of the CC certification matches the CRA scope of the product with digital elements in this type of products.**

Coverage of ESRs through SFRs and SARs in the PPs.

Reviewing and analysing all the SFRs and SARs of every PP mentioned in this section is exhaustive, so it will be done for a representative sample containing the example for the HSM defined in the PP [PP_CMCSOB]. The table below contains the exhaustive analysis:

[13] It needs to be clarified whether the server-side systems used by payment terminals need to be considered as remote data processing solutions from the perspective of the manufacturer of the payment terminal that needs to comply with CRA.

ESR	Required SFRs	Required SARs	Gap with mapping	Rationale	Conclusion
A I.1 (1)		ASE_SPD.1 Security problem definition ASE_OBJ.2 Security objectives ASE_REQ.1 Direct rationale security requirements	None		Compliant
A I.1 (2) (a)		AVA_VAN.1 Vulnerability survey	None		Compliant
A I.1 (2) (b)	FMT_SMF.1 Specification of Management Functions	ADV_ARC.2 Security Architecture with Default Secure Configuration (Extended)	FMT_SMF.1 Specification of Management Functions (with a management function to reset the TOE) ADV_ARC.2 Security architecture description	**Reset to default configuration**: the PP doesn't require this feature. => **GAP**. **Default Secure Configuration** is not in the PP, but the assumption "A.Trusted_Environment" imposes trusted administrators that shall configure the TOE according to the TOE guidance => **justifiable by risk assessment (SPD)**	Partially compliant*

A I.1 (2) (c)	EUCC patch mechanism with specific refinements.	SARs in EUCC patch mechanism evaluation methodology, with specific refinements.	SARs in EUCC patch mechanism evaluation methodology, with specific refinements.	The PP includes FPT_ITI.1 that ensures integrity and authenticity of updates through a secure channel, but doesn't impose any restrictions on the update mechanism itself (e.g., automatic, and opt-out mechanism). => **GAP** However, this type of device is used potentially in critical environments and for critical operations. Not using an automatic update mechanism and relying on the administrator to perform them might be justifiable, as the uptime and stability of the system is of importance. => **justifiable by risk assessment (SPD)**	**Partially compliant***
A I.1 (2) (d)	For identification and authentication: FIA_UID.1 or FIA_UID.2, and FIA_UAU.1 or FIA_UAU.2 For access management: FDP_ACC.1, FDP_ACF.1 For report on possible unauthorised access: FAU_GEN.1 Audit data generation and FAU_SAA.1 or FAU_STG.1		FAU_SAA.1 or FAU_STG.1	The report upon possible unauthorized access is actually implemented but modelled as an alarm to physical attacks (FPT_PHP.2 Notification of physical attack). **Therefore, the ESR is met through a different equivalent SFR suitable for this context.**	**Compliant***

A I.1 (2) (e)	Confidentiality of stored data: • FDP_SDC.21 Stored data confidentiality • FCS_COP.1 implementing memory encryption. • FDP_ACC.1 + FDP_ACF.1, and/or FDP_IFC.1 + FDP_IFF.1 for access control to memories or information flow control for stored data. • FPT_PHP.3 and/or FDP_ITT.1 and/or FPT_ITT.1 for protection against physical attacks and tampering (when attackers can physically access the TOE in high-assurance scenarios). Confidentiality of communications: FTP_ITC.1 Import of user data without security attributes, (between TOE and other IT entities), FTP_TRP.1 Trusted path (between the TOE and users) For cryptographic mechanisms used for the implementation any of the		without security attributes	**Data at rest:** it is not specifically protected in confidentiality with FDP_SDC.1, but stored data such as keys, user credentials, and backups etc. Using other mechanisms such as FCS_COP.1. **Data in-transit:** confidentiality protected with FTP_TRP.1 for communication with client application, FCS_COP to protect transferred backups. There is also an assumption for trusted channel with administrators and transferred updates don't need confidentiality protection. => **Justifiable by risk assessment (SPD)**	Compliant*

	above protections: FCS_COP.1 Cryptographic operation				

A I.1 (2) (f)	Integrity of data at rest and reporting corruption: either FDP_SDI.1+FAU_GEN.1 Audit data generation (registering event for corruption of data) or FDP_SDI.2 Integrity of communications: FTP_ITC.1 Inter-TSF trusted channel (between TOE and other IT entities), FTP_TRP.1 Trusted path] (between the TOE and users) For cryptographic mechanisms used for the implementation any of the above protections: FCS_COP.1 Cryptographic operation For particular reporting of integrity violation in each communication channel, FAU_GEN.1 Audit data generation.		FDP_SDI.1 FPT_ITC.1 Inter-TSF trusted channel	**Data at rest:** FDP_SDI.1 is not included but integrity of stored data is ensured through combination of cryptographic mechanisms of FCS class. **Violation of physical integrity** also addressed through FPT_FLS.1 Failure with preservation of secure state + FPT_PHP.2 Notification of physical attack and FPT_PHP.3 Resistance to physical attack **Data in transit:** FTP_ITC.1 is not included but FPT_ITI.1 protects integrity of the updates and backups in transit, and FTP_TRP.1 the trusted path with client applications. Communications with the human administrators are protected via assumption of the operational environment **(justifiable by SPD -> Risk assessment).**	**Compliant***
A I.1 (2) (g)		ADV_PDM.1: Processed Data Minimisation (Extended)	ADV_PDM.1		**Not Compliant**

A I.1 (2) (h)	FRU_FLT.1 Degraded fault tolerance FPT_FLS.1 Failure with preservation of secure state		FRU_FLT.1 Degraded fault tolerance	No tolerance to faults (FRU_FLT.1) regarding availability is implemented. However, a secure environment is assumed through the assumption "A.Trusted_Environment" which would make those type of attacks non-applicable and not meaningful in the scenario given in the PP => **justifiable by risk assessment (SPD).**	Compliant*
A I.1 (2) (i)	For minimization of impact in by product itself: FPT_INI.1 TSF initialization FPT_TST.1 TSF Testing For minimization of impact by connected devices: FDP_IFC.1 Subset information flow control FDP_IFF.1 Simple security attributes		FPT_INI.1 TSF initialization	FPT_INI.1 is not included but FPT_TST.1 includes execution of TSF self-test during initial start-up that, for the scenario given in the PP and the verifications done, are sufficient => **justifiable by risk assessment (SPD).**	Compliant*
A I.1 (2) (j)		AVA_VAN.1 Vulnerability survey ADV_FSP.1 Basic functional specification AGD_OPE.1 Operational user guidance	None		Compliant

A I.1 (2) (k)	FPT_FLS.1 Failure with preservation of secure state FPT_RCV.1 Manual recovery	AVA_VAN.1 Vulnerability survey ADV_TDS.1 Basic design ADV_FSP.1 Basic functional specification ADV_ARC.1 Security architecture description	FPT_RCV.1 Manual recovery	Upon a tampering event, the FPT_PHP and FPT_FLS components in the PP perform erasure of sensitive data. Manual recovery is needed. However, the security problem establishes assumptions including "OE.Recovery Secure Recovery" which requires a manual secure recovery upon incident by trusted administrators => **justifiable by risk assessment (SPD).**	**Compliant***
A I.1 (2) (l)	FAU_GEN.1 Audit data generation FMT_SMF.1 Specification of Management Functions FMT_SMR.1 Security roles		None		**Compliant**
A I.1 (2) (m)	For removal of data: FMT_SMF.1 Specification (with a function to delete data/settings) FDP_RIP.1 Subset residual information protection For transferring data: FMT_SMF.1 Specification (with a function to transfer data/settings) FDP_ETC.1 Export of user data without security attributes or FDP_ETC.2 Export of user data with security attributes FTP_ITC.1 Inter-TSF trusted channel		None of the required SFRs.	There is no manual mechanism for removal or export of user data or settings imposed by the PP.	**Not Compliant**
[redacted]					

A I.II (1)		ALC_FLR.1 ALC_SBM.1: Software bill of materials (Extended)	ALC_FLR.1 Basic flaw remediation ALC_SBM.2: Software bill of materials (Extended)		**Not Compliant**
A I.II (2)		Either one of: - ALC_FLR.1 Basic flaw remediation + SARs implementing the (technical) patch mechanism involved in EUCC's patch management procedure (ref. [ISO_TS_9569]) -ALC_FLR.3 Systematic flaw remediation and ALC_FLR.4 Flaw remediation with distinction between security and functional flaws (Extended).	None of the required SARs		**Not Compliant**
A I.II (3)		ALC_PSR.1 Periodic security review and testing	ALC_PSR.1		**Not Compliant**
A I.II (4)		ALC_FLR.1 Basic flaw remediation	None		**Not Compliant**
A I.II (5)		N/A			**Compliant**
A I.II (6)		ALC_FLR.2 Flaw reporting procedures	None		**Not Compliant**
A I.II (7)		Either one of: - ALC_FLR.1 Basic flaw remediation + SARs implementing the (technical) patch mechanism involved in EUCC's patch management procedure (ref. [ISO_TS_9569]) -ALC_FLR.3 Systematic flaw remediation	None of the required SARs		**Not Compliant**

A I.II (8)		Either one of: - ALC_FLR.1 Basic flaw remediation + SARs implementing the (technical) patch mechanism involved in EUCC's patch management procedure (ref. [ISO_TS_9569]) -ALC_FLR.3 Systematic flaw remediation	None of the required SARs		**Not Compliant**

Table 6 Coverage of ESRs in [PP_CMCSOB]

Paying attention to the column named “Gap with mapping”, it can be seen that 9/14 SFRs/SARs required, as per the mapping provided in this document, are not met. Moreover, none of the ESRs in Annex I.II are met also on the basis of the mapping.

However, further analysis provided in the column named “Rationale” goes deeper into analysing whether other SFRs or elements of the Security Problem Definition, e.g., the establishment of certain conditions (assumptions) of the environment where the TOE is deployed, lead to the conclusion that some of the ESRs are actually met (10/14) ESRs in Annex I.I become compliant* and 2/14 partially compliant), even when the mapping proposed in this study is not matched by the requirements in the PP. Those cases have been tagged in the table as **Compliant*** and **Partially compliant***.

This reinforces the argument given in previous sections that the mapping provided in this study is a proposal that doesn’t necessarily fit 100% of the cases. As can be seen in the example, the EUCC SPD can support the risk assessment in order to decide on the applicability of some of the ESRs and therefore (and it will be very usual) not all ESRs will be applicable for all types of products.

Even with this additional rationale, some ESRs in Annex I.I are still not met by the PP, and there is a gap that would need to be fulfilled. That gap could be addressed by updating the existing CC certifications out in the market (which could be replaced by certifications under EUCC scheme) by adding to them the CC technical elements (SFRs/SARs) that are required to meet the ESRS. In order to implement this bridge, a preliminary analysis would indicate that either the STs of products compliant with those PPs would need to be updated by applying one of the technical formulas proposed in the **ANNEX II: Options for implementation of CRA through EUCC technical elements in STs/PPs**”, or by updating the PPs when needed (**Section 7 Strategies for implementation in the industry** presents the implementation strategies in detail). In general, the PPs associated to this type of product don’t contemplate vulnerability and patch management procedures.

6.2.2. Smart meter gateways

In some smart metering systems, a specific smart meter gateway (SMGW) is a pivotal element[14], distinct from smart meters. It is a specialized firewall that bridges local devices within the consumer’s home area network (HAN) and metrological networks (communication network of the smart meters) and the wide area network (WAN). It processes, securely transmits and stores data, therefore providing a robust line of defence of the smart grid against potential cyber threats.

The security functionality of these smart meter gateways comprises in particular:

- The protection of data by ensuring confidentiality, authenticity, integrity, and
- the protection of the information flow between local and remote devices.

[14] The definition of the smart meter gateways and their security functionality included in this was elaborated by ESMIG (European association of smart energy solution providers) as a feedback response to an intermediate draft of this study.

They protect the privacy of consumers, ensure a reliable billing process and protect a smart metering system and corresponding large-scale infrastructures of the smart grid.

According to the definition provided by the European association of smart energy solution providers (ESMIG), a SMGW should provide the following functions:

1. Being capable of handling meter data from several types of smart meters (e.g. electricity, gas, water, etc.). It receives, stores and processes metering data from connected meters and uses this data to create billing relevant datasets protected by a digital signature
2. Ensuring privacy preservation and provides data only to eligible and authorized third parties (e.g., supplier, DSO, service provider, etc.)
3. Protection of authenticity, integrity and confidentiality of data temporarily or persistently stored in the device or transferred over the network interfaces of the device.
4. Firewalling of information flow between the WAN and the Home Area networks, e.g. information flow between meters, controllable systems (controllable energy loads, generators and storage devices) and the WAN.
5. The management of security functionality, e.g. certificate management, information flow, authorization of users or entities and connected devices.
6. The identification and authentication of users of the metering data stored in the SMGW (residential customers) or users of the control function of the SMGW (technical operators of the SMGW).
7. A key generation service for connected devices.

Additionally, the SMGW can support the information exchange between backend systems in the wide area network and devices connected to a Home Area Network via a transparent TLS proxy functionality.

The SMGW provides the ability to control local systems (e.g. energy loads, generators or storages) either via the TLS proxy or directly through a local interface. Therefore, the SMGW enables network operators to securely balance the energy grid based on the electricity network status and/or electricity market data. It enables the customer or an energy service provider to respond to energy market signals and optimize energy consumption.

Some smart meter gateways incorporate a security module that offers cryptographic services and secure storage for the gateway's operations. However, many smart meters don't have that module but integrated encryption and decryption functionality to realize end-to-end security with Head End Systems.

Protection Profiles

There are various protection profiles in the industry used for this type of products, being the more relevant the following that use high assurance requirements (EAL4+):

- Protection Profile for the Gateway of a Smart Metering System [PP_SMARTMETER_MSR] developed by the European Smart Metering Industry Group (ESMIG).
- Protection Profile for the Security Module of a Smart Metering System [PP_SMARTMETER_SM], which is specific for and scopes only the security module in those cases where the smart meter gateway incorporates such module.

For **all of these PPs**, the type of conformance required is **strict.**

Scope of the CC assessment

In the case of **Smart meter Gateway**, the TOE in scope of the CC TOE comprises the hardware and firmware that is relevant for the security functionality of the Gateway. In general, this matches with the full product.

The case of the **Smart meter security module,** it is typically an integrated circuit that is integrated within the hardware layer of the smart meter gateway. The smart meter also includes in the scope of the evaluation all the hardware and software required for the product to operate and doesn't include usually remote processing elements.

It must be noticed that the smart meter gateway and the security module are part of a more complex system, however this system itself is not contemplated in the category of critical products, which specifically scopes only the gateway.

As such, it can be concluded that for this type of products, **the scope of the CC certification matches the CRA scope of the product with digital elements in this type of products.**

Coverage of ESRs through SFRs and SARs in the PPs.

An exhaustive analysis of the coverage of the SFRs and SARs required for the mapping has not been performed for this type of technology, e.g., by reviewing if the PPs include the SFR/SARs that this study proposes to meet the ESRs in CRA Annex I, and by exhaustively analysing whether other technical elements in those PP could serve to meet those ESRs in an alternative manner, or the non-compliance with them can be compensated through the risk assessment linked to the CC Security Problem Definition.

However, a high-level analysis has been carried out in order to identify obvious gaps in the coverage of those SFRs/SARs in these PPs, and it has been identified that those PPs don't meet a number of the ESRs related to the following functionality:

i. Annex I.1 (2) (b): Secure configuration by default and reset to default configuration (but can be compensated by CC assumptions of trusted administration).
ii. Annex I.1 (2) (c): automatic updates.
iii.
iv. Annex I.1 (2) (g): data minimisation.
v. Annex I.1 (2) (m): removal of user data.
vi. Various of the ESRs in Annex I.2, as no SARs related to vulnerability management are included in these PPs.

6.2.3. Smartcards or similar devices, including secure elements

Smartcards are secure, tamper-resistant hardware devices used for various secure transactions and identity verification processes. They are integrated circuits that provide computational capabilities and secure storage for sensitive data, among other security features. In smart cards and similar devices, significant portions of the required security functionality depend upon hardware features at a chip level (for example smart card hardware/ICs, smart card composite products, TPMs used in Trusted Computing, digital tachograph cards, Hardware Security Modules, etc.). [EUCC] includes this domain as one being able to undergo EUCC evaluations with AVA_VAN.4 or AVA_VAN.5 and the protection profiles included in this sub-chapter are as already listed in [EUCC] Annex III.

In the certification industry they are assessed following the specific CC evaluation methodology that SOGIS develops for this type of technology in a specific technical domain (https://www.sogis.eu/)

provides specific guidance and criteria for the evaluation and certification of smartcards to ensure they meet high security standards.

Smartcard architecture usually comprises:

i. A hardware platform (Integrated Circuit) implementing hardware-based tamper resistant security mechanisms, such as and cryptographic operations and protection against physical attacks.
ii. An operating system, as firmware operating the hardware platform in a secure manner and providing libraries (e.g., cryptographic libraries) to upper application layers.
iii. Applications running on the top of the OS, such as payment application or identification (i.e. electronic passports), that use the security services exposed by the OS.

The image below taken from [SOGIS_SC_EVALUATION] depicts in a simplified manner the typical architecture of a smartcard:

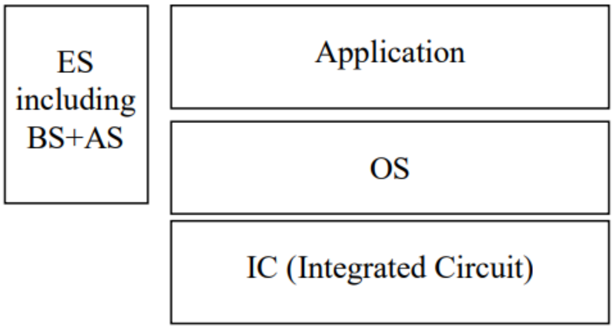


Figure 2 – Typical Smartcard architecture (Closed architecture)

Figure 22 Architecture of smartcard depicted in [SOGIS_SC_EVALUATION]

Protection Profiles

The following protection profiles are listed in SOGIS website as pertinent for this technical domain:

Passports:

- PP Machine Readable Travel Document using Standard Inspection Procedure with PACE **[PP_MRTD_PACE].**
- PP for a Machine Readable Travel Document with "ICAO Application" Extended Access Control **[PP_MRTD_EAC]**.
- PP for a Machine Readable Travel Document with "ICAO Application" Extended Access Control with PACE [**PP_MRTD_EAC_PACE].**
- PP for a Machine Readable Travel Document with "ICAO Application" Basic Access Control **[PP_MRTD_BAC].**

Secure Signature Creation Devices:

- PP for a Secure Signature Creation Device - Part 2: Device with key generation **[PP_SSCD_KG]**
- PP for a Secure Signature Creation Device - Part 3: Device with key import **[PP_SSCD_KI]**
- PP for a Secure Signature Creation Device - Part 4: Extension for device with key generation and trusted communication with certificate generation application **[PP_SSCD_KGCG]**

- PP for a Secure Signature Creation Device - Part 5: Extension for device with key generation and trusted communication with signature creation application **[PP_SSCD_KGSG]**
- PP for a Secure Signature Creation Device - Part 6: Extension for device with key import and trusted [**PP_SSCD_KISG].**

Digital Tachographs:

- Digital Tachograph - Tachograph Card **[PP_TACH_CARD]**

Security IC platform, OS and others:

- Security IC Platform PP **[PP_IC]**
- Java Card System - Open Configuration **[PP_JCOS_OPEN]**
- Java Card System - Closed Configuration **[PP_JCOS_CLOSED]**
- PP for a PC Client Specific Trusted Platform Module Family 2.0 Level 0 Revision 1.16 **[PP_TPM**
- Universal SIM card **[PP_SIM]**
- Embedded UICC (eUICC) for Machine-to-Machine Devices **[PP_eUICC]**

Scope of the CC assessment

The Protection Profiles used in the technical domain of the smartcard and similar elements can present several use cases regarding the scope of the CC TOE in the PP with respect to the scope of the product with digital elements.

In general, it must be stressed that some of the protection profiles of this technical domain address the certification requirements for the hardware platform, which would be the chip hardware (e.g., smartcard or security IC) including the firmware or software in it required to implement security mechanisms and provide services to upper layers.

Other protection profiles, such as those used in Java Card System, scope the Java Card runtime environment, virtual machine and APIs running on the top of the operating system of the smartcard hardware platform, that define an upper logical layer providing services to applications. These PPs require to perform a **composite evaluation** which would be an CC evaluation in which the TOE comprises an already certified HW platform (e.g., according to PP0084 [PP_IC]) integrated with the operating system. This situation can be also found in those PPs scoping the final applications running in smartcards, such as e-Passports, which are also approached as composite evaluations that reuse certified ICs and sometimes certified IC Platform Operating systems.

Regarding categorization of Java Card operating systems, it should be taken into account that an operating system per-se would not be considered a critical product under CRA. However, as they are generally placed on the market together with the underlying hardware platform, they are considered as part of a critical product under CRA.

The table below summarizes how each of those PPs cover fully or partially the scope of the product with digital elements:

PP	**Part of the architecture in scope of the EUCC**	**Scope of the assessment (full product or partial)**	**Relies on remote data processing elements (general case)**	**Notes**
[PP_MRTD_PACE] [PP_MRTD_EAC] [PP_MRTD_EAC_PACE] [PP_MRTD_BAC]	Machine Readable Travel Document (e.g., ePassport) application and optionally underlying OS. The scope requires a certified OS and IC platform.	Full (see notes)	**NO**	The PP requires a composite evaluation with an underlying certified IC platform and its OS. As a result, whole product is covered under the scope of the EUCC certifications of the different parts (IC, OS, Application)
[PP_SSCD_KG] [PP_SSCD_KI] [PP_SSCD_KGCG] [PP_SSCD_KICG]	Hardware and software implementing the signature creation	**Full**	**NO**	
[PP_TACH_CARD]	Tachograph application running on the top of a certified platform and OS.	**Full *** (see notes)	**NO**	Same as the case of the MRTD. Moreover, the other components in a vehicle tachograph system (Vehicle Unit, Gateway) are covered by the EUCC certification with other Protection Profiles (see previous section for Hardware Devices with Security Boxes).
[PP_TPM]	TPM device with associated firmware	**Full**	**NO**	
[PP_SIM]	SIM Software: Javacard System and Global Platform SW implementing uSIM APIs	**Full** * (see notes)	**NO**	The TOE scope in this PP doesn't include the underlying hardware. But the PP assumes a Security IC certified against an EUCC smartcard protection profile. Therefore, the whole solution would be certified
[PP_eUICC]	Software that implements the GSMA Remote	**Full** * (see notes)	**NO**	The PP doesn't include in-TOE scope the underlying platform and OS. However, the Security Problem in the PP requires that these

	Provisioning Architecture for Embedded UICC Technical Specification [GSMA_UICC]. (Application layer)			components are certified against platform-related PPs. Therefore, the whole solution would be EUCC-certified.
[PP_IC]	Hardware platform (IC) and its embedded software	**Full** * (see notes)	**NO**	The IC certified against this PP is put in the market corresponds in general with the full security chip. Therefore, the whole solution would be EUCC-certified.
[PP_JCOS_OPEN] [PP_JCOS_CLOSED]	Javacard OS running on the top of a certified HW platform	**Full** * (see notes)	**NO**	This PP requires a certified HW platform using to one of the platform-related PPs. Therefore, the whole solution would be EUCC-certified.

Table 7 Smartcard PPs analysis

Coverage of ESRs through SFRs and SARs in the PPs.

A detailed exploration of the coverage of ESRs would require an in-depth exhaustive review of all the aforementioned Protection Profiles that goes beyond the scope of this study. A sample has been done examining these protection profiles and, at a high level, lack of coverage of the following ESRs:

i. Annex I.1 (2) (b): Secure configuration by default and reset to default configuration (but can be justified as non-applicable based on CC assumptions of trusted administration).
ii. Annex I.1 (2) (c): automatic updates.
iii. Annex I.1 (2) (g): data minimisation.
iv. Annex I.1 (2) (i), protection of availability of services of the product and other products in the network.
v. Annex I.1 (2) (m), removal of user data on-demand.
vi. Various of the ESRs in Annex I.2, as no SARs related to vulnerability management are included in some of these PPs.

6.2.4. Conclusions for critical products

The following comparative table provides a summary of the analysis performed for the key aspects of the PPs in the market that impact the how to meet with the CRA ESRs through EUCC, according to the analysis performed so far.

In the last column, the terms related to coverage mean the following:

- *Direct coverage:* SFRs/SARs in the PP that directly address the CRA ESRs, as per the mapping proposed in this study.
- *Indirect coverage:* there are other SFRs or SARs different from those proposed in the mapping included in this study that may satisfy the related CRA ESRs, or it can be assumed that some of the ESRs would not be applicable for the product.

Type of critical product	PP conformance required in typical PPs	Scope of the EUCC assessment vs CRA product with digital elements	Requires remote data processing solutions (General case)	Coverage of required SFRs /SARs for CRA conformance
Hardware devices with security boxes	Strict	full product	NO[15]	Direct coverage: low Indirect coverage: high but not complete With gaps Gaps in vulnerability management-related requirements.

[15] It is required to clarify whether and in which cases, the server-side payment systems utilized by payment terminals are considered remote data processing solutions from the perspective of the manufacturer of the payment terminal.

Smart Meter Gateways	**Strict**	Full product (as a part of a non-certifiable complex system)	**NO**	Direct coverage: low Indirect coverage: high but not complete **With gaps**
Smartcards and similar devices	**Strict** Demonstrable (depending on the PP)	Full product (with composite evaluations for layers on HW, e.g., applets)	**NO**	Direct coverage: low Indirect coverage: high but not complete **With gaps**

Table 8 Summary for critical products

The conclusions that can be drawn for Critical products are as follows:

1. A high number of high-assurance PPs exist in the industry for CC certification of this type of components, often regulated by technical domains (aligned with those technical domains in EUCC) and other regulations. Certification of this type of devices without a PP almost doesn't exist in the industry.
2. PPs used for products of this category require strict conformance or demonstrable conformance, hence they could be interoperable with some of the options proposed in **"ANNEX II: Options for implementation of CRA through EUCC technical elements in STs/PPs"** of the Annex to this document.
3. There is certain degree of gap in the direct coverage of SFRs and SARs required for CRA compliance, as proposed in this study. However, further analysis of each PP requirements and of the elements in the SPD in it offers a reasonable path to demonstrate conformity with a high percentage of ESRs of Annex I Part I of CRA. Some of the security concerns meaningful for the product are often addressed through an alternative strategy (e.g., relevance of assets, elements in the environment, alternative SFRs for protection of the assets obtaining the same result) that also result in conformance with the ESR. Alternatively, some of the ESRs in CRA Annex I Part I are simply not applicable for the security problem given. This would be equivalent to elaborating on the **manufacturer's risk assessment to perform the adequate selection of ESRs.** it should be taken into consideration that the protection profiles associated with these product categories support high assurance EUCC evaluations. Based on the risk scenarios and attacker profiles established in these profiles, and given the maturity of the certification industry in terms of the associated technical domains, it could be said that the evaluations of these types of products are among those that offer the highest security assurance in the certification market. As such, the selection of SFRs and SARs included in those PPs should be sufficient with respect to the protection of the solution in the foreseen risk scenario and, although a case-by-case analysis could be necessary, in general no additional security requirements would be needed in them and, therefore, the ESRs not covered by them could be probably justified as non-applicable.

   With regards to **ESRs in Annex I Part II**, these are not conditional to the result of the manufacturer's risk assessment and must be complied with in all cases, even while following a risk-based approach for some of them. The ESRs in Part II of the CRA Annex II refer to manufacturer processes related to vulnerability handling and, in the cases where gaps are found in the compliance with such ESRs, it might be required to add, either via updates of the related PPs or in PP-compliant STs those technical elements (SARs, SFRs) of EUCC that don't exist currently in the PPs but are necessary in order to provide compliance with this group of ESRs.

In the light of these data, it can be concluded that the gap of the PPs used in the certification of the main types of Critical products with digital elements (according to annex IV of CRA) is small **if it is combined with an adequate analysis (justifying through risk assessment –SPD) that the security features included in the evaluation of these devices are enough to provide the necessary level of protection to their relevant assets in the intended use scenario and, therefore, in functional terms, it can be justified that no all ESRs in CRA Annex I, part 1 (and therefore SFRs / SARs) need to be complied with in these PPs.**

Therefore, the gaps can be addressed by:

1. **Justification of applicability of ESRs in Annex I, Part I,** indicating that the SFRs/SARs currently present in the PPs are sufficient on the basis of the risk assessment linked to the SPD.
2. Where gaps in the compliance with ESRs of Annex I Part I are found and can't be justified through risk analysis, or gaps exist in the compliance with ESRs in Annex I, Part II, then **the protection profiles should be updated progressively to include those SFRs and SARs that cover the remaining CRA ESRs.**

6.3. Important products with digital elements

Annex III of CRA defines two classes of Important products, Class I and Class II depending on the risk level derived from a potential adverse effect. This section aims to identify which Protection Profiles in the industry are currently used to certify each category of product and, where a PP is used, it is analysed if their ST-compliant STs could be updated with additional technical elements (SFRs/SARs) as needed in order to ensure that CRA ESRs are complied with through their certification. Since the list of products categories in Annex III is quite extensive, no deep analysis is performed individually for all the categories.

The product categories in Annex III of the CRA encompass a wide range, leading to a diverse set of Protection Profiles used in the industry for CC certification of these products. Some product categories include non-security products that implement security functions, which means their certification is not widely adopted in the industry. Consequently, there may be no existing Protection Profiles in the market that cover these types of products. For those cases, the use of PPs don't constraint the technical mechanisms (see section **7 Strategies for implementation in the industry**) that could be used to incorporate in them the additional SFRs and SARs required for compliance with the CRA ESRs that have been identified and proposed in this study. This means that there is full flexibility in how to incorporate those CC technical elements in the market, e.g., by using CRA-Tailored STs or protection profiles.

The table below presents a detailed analysis for each type of important product as in CRA Annex III on what would be the impact in the event that a gap is found in the industry mainstream PPs used to certify that category of product. The table takes into account the following factors:

- Column 1: the **type of important** product with digital elements according to CRA Annex II.
- Column 2: widespread **protection profiles** that are or could be potentially employed for the certification of the CRA product category, along with the **type of compliance** (strict, demonstrable or exact) set out in those PPs and the assurance level of the PP.

- Note: not all PPs in the market that could be used to certify products of a certain CRA category are included in the table. This study picks a sample of one or more PPs (when available) that are representative or meaningful for each category in the table.

- Column 3: whether the scope of the certification covers the full product when use those mainstream PPs. Possible values are:
  - **Full product,** if the PP targets the full product with digital elements as TOE boundary.
  - **Subset of product** if the scope of the TOE defined in the PP is different from the scope of the full product with digital elements.
- Column 4: for each PP listed in column 2, whether the PP defines a TOE that relies on non-TOE remote IT entities that could fit in the definition of remote data processing elements.
- Column 5 : a global verdict , taking account the PPs listed in column 2 for the product category, whether, in the event that one or more of the PPs don't meet all the CRA Annex I ESRs through equivalent SFRs/SARs, the a ST compliant with that PP could be updated by adding those additional SFRs/SARs in order to close gaps in the compliance with CRA ESRs (instead of updating the PP). Possible values are:
  - **Allowed by PP conformance**, the PPs identified in column 2 allow additional SFRs/SARs in a PP-compliant ST, or if no PP has been identified for the category.
  - **Not allowed by PP conformance**, the PPs identified in column 2 don't allow additional SFRs/SARs in a PP-compliant ST
  - **Case-dependent**, depending on which PP is used to certify that type of product, the PPs identified in column 2 may allow or not additional SFRs/SARs in a PP-compliant ST

The aim of this table is to illustrate how the listed PPs, as they are in the market at the date of publication of this report without further modifications, would allow to demonstrate that the PP-compliant product in an EUCC certification would meet the CRA ESRs or if, in case of gaps, they would allow per-ST updates carried out on a per-product basis by manufacturers in order to fill those gaps.

For example, a PP that would allow to comply with CRA through CC would show in the table as:

1) "**strict**", "**demonstrable**" or "**No PP**" in the first column.
2) "**Full product**" in the third column.
3) "**NO**" in the fourth column.
4) "**Allowed by PP conformance**" in the third column.

Otherwise, the compliance of that type of product when EUCC-certified using one of its identified PPs wouldn't be direct and the specific case would need to be analysed.

Class I important products				
Product type	**Existing protection profiles / Conformance (strict | demonstrable | exact)**	**Typical scope of the certification (Full product | Subset of product)**	**Requires remote data processing solutions (YES | NO | Possibly)**	**Feasible to meet CRA for the full product in the current situation, if additional SFRs/SARs need to be added** **PPs allow to modify the PP-compliant ST to close gaps in**

				compliance with CRA ESRs by adding SFRs/SARs to the ST. (Allowed by PP conformance / Not allowed by PP conformance / Case-dependent)
1. Identity management systems and privileged access management software and hardware, including authentication and access control readers, including biometric readers;	**Software modality (in general):** [PP_APPSW] / **exact** conformance / below EAL1	**Full product**	**Possibly**	**Case-dependent**
	Hardware modality (in general): [CPP_ND] / **exact** conformance/ EAL1	**Full product**	**Possibly**	
	Access control readers: Protection Profile for Peripheral Sharing Device Version + PP-Module for User Authentication Devices / **exact** conformance / EAL1	**Full product**	**No**	
	Hardware reader Secure Smartcard Reader with Human Interface Protection Profile / **demonstrable** conformance / EAL3+	**Full product**	**No**	

	Biometric HW readers: No PP currently in the market	**Full product** (as per ST-author definition)	**No** (as per ST-author definition)	
2. Standalone and embedded browsers;	**No PP** or [PP_APPSW] / **exact** conformance / EAL1 Note: no products of this type certified so far but [PP_APPSW] would be a suitable option.	**Full product:** The scope of the solution is limited to the browser.	**NO**	**Case-dependent**
3. Password managers;	**No PP** or [PP_APPSW] / **exact** conformance / EAL1 Note: no products of this type certified so far but [PP_APPSW] would be a suitable option.	**Full product:** password managers in the market are usually deployed as standalone desktop/mobile applications.	**NO**	**Case-dependent**
4. Software that searches for, removes, or quarantines malicious software;	**Server:** [PP_APPSW] + PP-Module for Endpoint Detection and Response / **exact** conformance / EAL1	**Full product:** including agent and console in two separate certifications.	**NO**	**Not allowed by PP conformance**

	Client: [PP_APPSW] + PP-Module for Host Agent / **exact** conformance / EAL1	**Full product:** including agent and console in two separate certifications OR **Subset of product in Non-corporate case** (standalone endpoint without central console)	**YES** In non-enterprise cases, servers with definition of threat databases are cloud-hosted.	
5. Products with digital elements with the function of virtual private network (VPN);	Extended Package for VPN Gateway / **exact** / EAL1 PP-Module for Virtual Private Network (VPN) / **exact** conformance / EAL1	**Full product:** full HW appliance in HW devices, full SW program in SW cases	**NO**	**Not allowed by PP conformance**
6. Network management systems;	**Software modality:** **No PP** or [PP_APPSW] / **exact** conformance / EAL1	**Full product**	**NO**	**Case-dependent**
	Hardware modality: **No PP** or [CPP_ND] / **exact** conformance / EAL1	**Full product**	**NO**	
7. Security information and event management (SIEM) systems;	**Software modality:** **No PP** or [PP_APPSW] / **exact**	**Full product: (on-premise deployment)**	**YES (frequently)** Server-side dashboard +	**Case-dependent**

	conformance / EAL1 **Hardware modality:** **No PP** or [CPP_ND] / **exact** conformance / EAL1	**Subset of product:** **(cloud-based)** SIEM architecture typically consists of an agent, a sensor, both installed in-house, and a centralized administration console or dashboard, deployed in-house or in the cloud. The three above components can be certified together, in a single evaluation, when they are deployed in-house.	event analysis server typically hosted in-the-cloud	
8. Boot managers;	**No PP:** No certified cases found during this study	**Full product** Typical deployment consists in two software components, a server and an agent. Both are necessary for operation and are part of the same product.	**NO**	**Allowed by PP conformance** (no PP)
9. Public key infrastructure and digital certificate issuance software;	Certificate Issuing and Management Components Protection Profile / **demonstrable** / EAL4+ALC_FLR.2	**Subset of product:** the PP doesn't include in-scope the cryptographic module used to perform cryptographic operations	**YES** Potentially For PKI or digital certificate issuers running in the cloud, part of the infrastructure cloud-hosted.	**Not allowed by PP conformance**

9[16]. Physical and virtual network interfaces;	**No PP** Note: some PPs in the market would cover a TOE encompassing a physical or virtual network interface as part of a larger TOE, but there isn't currently a dedicated PP for the interface alone	**Full product** (Choice of the ST author)	**Possibly** i.e., cloud-administered devices	**Allowed by PP conformance** (no PP)
10. Operating systems;	[PP_OS] / **exact** conformance / EAL1	**Subset of product:** Not all parts of the OS are necessarily included in the certification	**NO**	**Case-dependent** If [PP_OS] is used, no additional SFRs/SARs can be added due to exact conformance. If [PP_ETSI_CMD] is used, demonstrable conformance would allow it. (Note: the scope of [PP_ETSI_CMD] is the full mobile device plus its firmware and software, including the operating system, but demonstrable conformance would allow limitation of the scope in justified cases.
	[PP_ETSI_CMD] (in the case of mobile device operating systems) / **demonstrable** / EAL3 + ALC_FLR.3	**Subset of product:** Not all parts of the OS are necessarily included in the certification	**NO**	
11. Routers, modems intended for the connection to the internet, and switches	[CPP_ND] / **exact** conformance / EAL1	**Full product** The PP requires the full appliance to be in-scope.	**Possibly** Several cases in the industry use cloud-hosted management servers/consoles for device administration.	**Not allowed by PP conformance**
12. Microprocessors	**No PP**	**Full product**	**NO**	**Allowed by PP conformance** (no PP)

[16] The number 9 in the enumeration OF important products with digital elements of Class I appears twice in the latest text of the CRA (https://www.europarl.europa.eu/doceo/document/TA-9-2024-0130_EN.html#title2) and seems to be an errata.

with security-related functionalities	No certified cases found during this study	Microprocessors in general are standalone products deployed in devices under the control of the customer, and the environment can be reproduced and controlled by ITSEFs.		
13. Microcontrollers with security-related functionalities;	**No PP** No certified cases found during this study	**Full product** Microcontrollers in general are standalone products deployed in devices under the control of the customer, and the environment can be reproduced and controlled by ITSEFs.	**NO**	**Allowed by PP conformance** (no PP)
14. Application specific integrated circuits (ASIC) and field-programmable gate arrays (FPGA) with security-related functionalities;	**No PP**	**Full product** Generally, the ASIC is a self-contained HW component	**NO**	**Feasible**
Class II important products				
Product type	**Existing protection profiles / Conformance (strict | demonstrable | exact)**	**Typical scope of the certification (Full product | Subset of product)**	**Requires remote data processing solutions (YES | NO)**	**Feasible to meet CRA for the full product in the current situation, if additional SFRs/SARs need to be added**

				PPs allow to modify the PP-compliant ST to close gaps in compliance with CRA ESRs by adding SFRs/SARs to the ST. (Allowed by PP conformance / Not allowed by PP conformance / Case-dependent)
1. Hypervisors and container runtime systems that support virtualised execution of operating systems and similar environments;	Protection Profile for Virtualization / **exact** conformance / EAL1	**Full product:** includes the full software virtualization system	**NO**	**Not allowed by PP conformance**
2. Firewalls, intrusion detection and prevention systems;	[CPP_ND] / **exact** conformance / EAL1	**Full product** The PP requires the full appliance to be in-scope.	**Possibly** Several cases in the industry use cloud-hosted management servers/consoles for device administration.	**Not allowed by PP conformance**
3. Tamper-resistant microprocessors;	**No PP**	**Full product** The full microprocessor should be in-scope of the certification.	**NO**	**Allowed by PP conformance** (no PP)
4. Tamper-resistant microcontrollers.	**No PP**	**Full product** The full microprocessor should be in-scope of the certification.	**NO**	**Allowed by PP conformance** (no PP)

Table 9 Impact analysis of gaps for important products with digital elements

The study on various significant products with digital elements, classified under classes I and II, extensively utilizes protection profiles, particularly [CPP_ND] and [PP_APPSW], both of which rank among the top-10 PPs in five-year statistics. However, the industry has not yet developed a mainstream protection profile for certain types of products in the list. The predominance of these protection profiles suggests that a significant portion of these products are certified using exact conformance PPs. Under that situation, the exact conformance wouldn't permit manufacturers to modify the PP-compliant STs (i.e., to add SFRs/SARs that would help to meet the CRA ESRs) on a per-product basis, and using those PPs with exact conformance **would require to review and update the PPs through the dedicated technical committees** (see explanation of the concept in section **4.4 Other relevant elements in EUCC/CC**).

Regarding the scope of the EUCC certification, when a PP is utilized, the certification scope often encompasses the entire product, aligning with the scope of the product with digital elements. In cases where no PPs are used, this comprehensive coverage is not guaranteed. Moreover, some PPs, such as [PP_OS], do not yet cover the full product in their assessment scope. In summary, certain PPs used for CC certification of important products with digital elements require the full scope of the product to be in the full scope, whereas other PPs design a TOE scope narrower than the full product scope.

Additionally, many of these products rely on remote data processing services for their operation, such as network devices with administration consoles or endpoint software that requires remote servers for functions like threat or adverse event databases. In these cases, the certification scope includes securing communications with such remote elements but not the remote elements themselves.

Since the number of PPs used to certify this solution is elevated, this study hasn't performed an in-depth analysis of every one of them in order to verify the degree of coverage of essential security requirements (ESRs) from CRA Annex I. However, doing a high-level overview and some degree of sampling, it can be easily concluded that, in general, these PPs don't include the necessary CC SFRs/SARs corresponding with the CRA ESRs. Taking as an example the most used ones for these categories of products, [CPP_ND] and [PP_APPSW], they present gaps **at least** in the coverage of the following ESRs:

- Annex I.1 (2) (b): Secure configuration by default and reset to default configuration (but can be compensated by CC assumptions of trusted administration).
- Annex I.1 (2) (c): automatic updates.
- Annex I.1 (2) (g): data minimisation.
- Annex I.1 (2) (k) regarding self-tests and protection against incidents.
- Annex I.1 (2) (i), protection of availability of services of the product and other products in the network.
- Annex I.1 (2) (m), removal of user data on-demand.
- Various of the ESRs in Annex I.2, as no SARs related to vulnerability management are included in these PPs.

In general, some requirements introduced by the CRA that weren't traditionally common in the CC industry, such as "minimization of data," are often needed for many significant products but are not yet established in the industry. Also, PPs such as [CPP_ND], [PP_APPSW] and [PP_OS] are low assurance (EAL1 with AVA_VAN.1) and they would fail to meet various SFRs identified in the mapping provided in section **5.1 Complying with CRA ESRs Annex I, Part I through EUCC technical elements**, due to the low assurance package, i.e., ADV_ARC.1 Security architecture description.

In certain cases, it might be justified that the security problem addressed by the PP renders the ESR unnecessary, but this might not always be the case.

Therefore, there will generally be a need to add new technical elements (SFRs/SARs) to these PPs in order to meet with the CRA ESRs that, for those PPs requiring exact conformance, would involve review and update of the PP as the only option.

Also, with regards to technical the options for implementation of CRA through EUCC (i.e., as a tool to include additional SFRs/SARs in certifications), it is important to consider the exploration that this study performs in section **"ANNEX II: Options for implementation of CRA through EUCC technical elements in STs/PPs"** of the Annex to this document. That part of the study shows that those implementation strategies (generic PP, PP-configurations, etc.) aren't very practical or easy to implement if the intention is to apply them to PP-compliant STs and they are further limited when the PPs require exact conformance.

On the other hand, some of the product's types in the table have been identified as having CC TOE scope different from that in the product from digital elements, or having remote data processing elements, that might also make it more difficult to meet the CRA ESRs through EUCC only. The option to address this situation through multi-assurance PP-configurations would require a deep update of the structure of the PPs mentioned in this subchapter.

Under this scenario, considering the usage of the PPs identified in the previous table:

- For 4/14 categories of important products in class I meeting the CRA requirements through EUCC could be more difficult (but 4 of them are CC certified using widely-spread protection profiles in the top-10 statistic), and 7/14 of them could be obtaining depending on a per-case basis.
- 2/14 categories of important products in class II could not meet the CRA requirements through EUCC.

This means that, for the industry share of products that are certified using the Application Software PP [PP_APPSW] and the Collaborative Protection Profile for Network Devices [CPP_ND], **which are the third and fifth most used PPs in the industry in the latest years, when additional SFRs or SARs need to be added to the scope of the evaluation to obtain CRA compliance, a revision of such cPPs would be needed to support obtaining CRA conformance through EUCC evaluations when such PPs are used.**

Another relevant situation needs to be highlighted. The most frequently used protection profile [CPP_HARDCOPY] corresponds to multi-function devices such as printers/scanners. **This type of product that has a large share in the certification industry is not included in any of the categories of important devices of CRA.** This situation illustrates certain cases in which certain types of products that aren't included in the CRA list of critical or important products with digital elements, but still their certification under CC is a widespread practice in the industry. Although the case of the hardcopy devices is the most noteworthy**,** yet **there are other types of products that can still meet the CRA requirements through CC certifications that are already on the market**. It might be required to further survey the certification marked in search of other cases like this one, that could potentially motivate a future update in the list of product categories contemplated by CRA in order to enlarge and enrich it.

7. Strategies for implementation in the industry

The previous sections examined the technical aspects necessary for EUCC certifications to meet CRA requirements, including methods for implementing these aspects in Security Targets (STs) and Protection Profiles (PPs). Additionally, the sections analysed the certification landscape, assessing the implementation options within the current CC certification industry.

When combining all these elements, the study identified several considerations, which are summarized as follows:

1. **The security aspects described in some CRA ESRs aren't addressed by CC technical elements existing in the industry.** For example, not the CC standard, nor any of the existing CC certifications in the market cover the security concern of the "data minimisation". In order to close this gap, the PPs and/or STs must be updated by including, where necessary, extended SFRs/SARs designed ad-hoc for this purpose, or SFRs/SARs that exist in the CC standard but are not included in the relevant PPs/STs. In the future, it could be considered to include such extended requirements in the CC standard.

2. **Possible challenges in implementing the technical elements required to bridge the gap between EUCC and CRA certifications in the market.** A high number of certifications are carried out using STs compliant to PPs and many of those use exact conformance PPs.
   In the Annex to this study, section **"Annex II: Options for implementation of CRA through EUCC technical elements in STs/PPs**" explores different technical options on how to include those SFRs and SARs required to meet the CRA ESRs in EUCC certifications, considering two scenarios: when the EUCC ST claims conformity to PPs in the market (interoperability) and when it doesn't. A summary of those options is presented in the table below:

Option	Description
CRA-tailored (standalone) security target	Drafting of a STs that are not compliant to any PPs and they are tailored in a way that include the SFRs and SARs that are required to meet the CRA ESRs. While there is high flexibility and freedom on the incorporation of the technical elements to the ST, only 23% of the manufactures don't use PPs. Manufacturers prefer the use of PPs to promote a harmonised approach across the industry.
Protection-Profile tailored for CRA conformance	Drafting a generalist protection profile that includes the SFRs and SARs required to meet the CRA ESRs. STs claiming conformance with this ST would meet the ESRs as well. This option provides a high level of harmonization for manufacturers and CABs, but the creation of a technology-agnostic PP is not easy. Can't be used with STs that claim conformance with PPs with exact conformance, and for the rest of PPs may have a duplication of the SFR and SARs. However, a generalist PP for all types of products could result too large, complex and perhaps unpractical.

PP-Configuration - Modular PP(s) with PP-Modules	One PP with modular parts modelled by PP-modules. Related functionalities described by CRA ESRs would be organized into PP-modules (i.e., secure communications, protection of stored data, etc.) and they would include SFRs and other technical elements related to those ESRs. PP-configurations are predetermined finite combinations of PP-modules existing in the PP. The level of harmonization would be high, while flexibility for specific use cases would be high due to PP-modules. However, flexibility would be limited to the existing finite number of PP-module combinations (PP-configurations). Complexity could potentially be high. As with the previous case interoperability with STs that claim conformance with other PPs could be difficult.
Standalone functional and assurance packages	Packages contain sets of SFRs (functional) and SARs (assurance) and can be defined in a modular and reusable way. They can be included in standalone STs, PPs or PP-modules. High flexibility and good level of interoperability with PP-compliant certifications (except when exact conformance is used). Moderate level of harmonisation. The PPs with exact conformance will need to be updated to include these packages.
PP with functional packages	Definition of one or more PPs that claim conformance with functional and assurance packages that include the SFRs and SARs required to comply with the CRA ESRs. High balance between flexibility and harmonisation. Interoperability with PP-compliant certifications is limited to those that don't use exact conformance. The PPs with exact conformance will need to be updated to include these packages.

Table 10: options for implementation CRA ESRs through EUCC technical elements

The analysis performed in the Annex shows that when conformance with other PPs is claimed, these options may result that interoperability can't be achieved with exact conformance PPs. As such, this study has chosen to dismiss the above options in scenarios where critical or important products are certified using other PPs in the industry, in favour of a strategy consisting in updating those PPs to ensure that they can be used to meet CRA.

3. **Mismatch between the scope of the TOE in the EUCC certification and the scope of the product with digital elements** in certain market cases, where the scope of the TOE is smaller and certain parts of the product wouldn't be covered by the scope of the certification, thus, in the current version EUCC wouldn't provide any assurance on the compliance of those parts with the CRA ESRs.

4. **Unsuitability of EUCC for covering remote data processing** solutions in the scope of the certification, as EUCC in its current version, doesn't support evaluation of products hosted in the cloud.

The rest of the sub-chapters in this section weigh a series of factors that need to be taken into account when making a decision on how to address these gaps.

7.1. Impact of the legislation in the industry

The study showed that there are theoretical ways to design the implementation of CRA through technical elements under EUCC scheme, using CC standard, with a wide range of tools to make the standard flexible and extensible to great variety of technological solutions. The analysis of the options and their feasibility also requires to take into consideration market realities.

This study also acknowledges that the CC certification industry, both in Europe and globally, has reached a state of maturity and consolidation. More than a decade ago, key technical communities, leading manufacturers, and national entities embarked on a journey to lay the groundwork for the present state of the industry. Their collective efforts have been dedicated to meticulously investigating and defining the mature aspects of CC that will persist under EUCC. This endeavour has involved the establishment of technical domains and the development of over 300 active protection profiles, requiring intensive engagement from various stakeholders and Member States.

Behind each type of technological product and its protection profile, there has been a period of study, discussion, development of technical elements, industry approval, and validation, culminating in final approval by ITSEFs, NCCAs, and the market at large. Every established CC certification strategy in the market represents a significant effort from multiple stakeholders.

Today, certification processes in the Common Criteria market are typically costly and demand significantly high amounts of time and effort. Depending on the chosen Evaluation Assurance Level (EAL), a certification process can span between 6 to 18 months. Throughout this period, the manufacturer must allocate extensive resources to provide ongoing support for the certification process and, subsequently, for its maintenance. In addition, each SFR or SAR required will involve an increase on the cost and time for the manufacturer and also more workload to the few overload CABs that are available. At the same time, Common Criteria certification is at the beginning of a new era with the EUCC and the Cyber Resilience Act, which requires industry to think their CC strategies considering this context.

It's undeniable that the industry must adapt to comply with CRA legislation, that is expected to be fully applicable as of 2027 (following a 36 months transition period). Therefore, it is at in the industry’s best interest to start thinking early on possible implementation strategies. Within the technical scope explored in this study, there are some options that could be implemented in a harmonized manner taking into account market realities and following a gradual and progressive strategy.

Following this, some pathways for demonstrating compliance with CRA through EUCC are proposed, considering the current state of certification in the existing landscape.

7.2. Harmonised CRA implementation through PP reviews and updates

The strategy proposed in this study revolves around the reuse of the mainstream PPs that are currently used in the CC certification industry. During the present transition period from CC Version 3.1 revision to CC 2022 revision 1, with the publication of the EUCC Implementing Act [EUCC] and the future entry into force of the CRA, a window of opportunity appears for relevant stakeholders to update the PPs as needed where they present gaps in the compliance with the essential requirements of the CRA.

The study has showed so far that, given the maturity and the guarantee offered by future EUCC certifications, they can demonstrate the compliance of ICT products with CRA ESRs provided that an equivalence relationship (mapping) between those ESRs and the CC SFRs/SARs in the evaluation is found. Moreover, the selection of SFRs and SARs in EUCC is originated in a risk assessment process (Security Problem Definition) in a manner similar to that in the CRA, where the ESRs in Annex I, Part 1 are selected by the manufacturer based on a risk assessment process as well.

Several CC PPs widely used in the industry present gaps in the compliance with the CRA ESRs (i.e., some ESRs aren't included in CC PPs by equivalent SFRs or SARs). PPs can be reviewed in order to analyse, by a thorough examination of the Security Problem Definition, the security features described by ESRs in CRA Annex I, Part 1 can be deemed and justified as not applicable for risk assessment associated to the particular SPD in each specific PP. This way, **manufacturers can justify, in some cases, that no other SFRs/SARs than those already included in the PP are needed for that particular SPD**. As a way to formally report such applicability analysis (a.k.a. ***Statement of Applicability***), this study proposes the use of the template provided in section **"Annex III. Template: CRA conformance claims for EUCC certified products"**

Note: the applicability of the ESRs in CRA Annex I, Part II is not dependent on or conditional to the result of the manufacturer's risk assessment. These need to be complied with in all cases.

At the same time, **PPs are a great tool for providing harmonization** to the certification industry, as they release manufacturers from elaborating individual per-product analysis (i.e., analysis of the SPD, selection of SFRs/SARs), and removes from CABs the burden of analysing the consistency and completeness of those same technical aspects in an individual based when a PP is used. In the same way, they can provide harmonisation for the introduction of technical elements in EUCC evaluations aimed to meet the CRA ESRs, such as the risk analysis based in the SPD, the selection of the ESRs, and even the justification of ESR applicability (a.k.a. Statement of Applicability previously mentioned), that can be reused in every PP-compliant evaluation.

This study also proposes the use of the template provided in section **"Annex III. Template: CRA conformance claims for EUCC certified products"** to support manufacturers in performing various claims related to conformity with CRA in ongoing and future EUCC evaluations.

PPs can provide harmonization not only in the ways in they can justify that they may already meet the CRA ESRs based on their existing technical elements together with their SPD. **When a PP doesn't meet as is some of the CRA essential requirements, it can be updated to close such gaps.** These updates may consist in additions of SFRs and/or SARs, along with linked modifications in certain elements of the Security Problem Definition that relate to those SFRs/SARs. These modifications should be accompanied of the template given **"Annex III. Template: CRA conformance claims for EUCC certified products"** where the appropriate claims related to CRA essential requirements shall be done.

In those EUCC PPs where it can be demonstrated the compliance with the CRA ESRs, either through an update of the PP or through justification of the compliance of its existing elements, future EUCC certifications of products compliant to that PP will guarantee that the products certified in compliance with that PP also meets the CRA ESRs. Again, this circumstance provides a considerable level of harmonisation.

In the particular case of the collaborative Protection Profiles maintained outside of the EU, their equivalent assurance level is usually below EAL2, i.e. not including design or security architecture review activities in the scope of the evaluation, they might present a larger gap in fulfilling the CRA ESRs than other Protection Profiles. These PPs are used to certify non-critical products outside the EU, but a large portion of such products are widely sold within Europe (i.e., network devices) and they will need to comply with CRA. The 2012 CCRA Vision Statement[17] emphasizes the need to raise general ICT COTS security levels without harming price or availability. It remains to be seen if such collaborative Protection Profiles maintained outside of the EU will be gradually updated. Future updates of those PPs might find ways to either address currently existing gaps or to justify that their threat model and security proposal is sufficient to the extent of the risk scenario they are designed to address. Such updates might contribute to use those PPs ways as a direct to comply with CRA ESRs for products certified in compliance with them. In the hypothetical event that a portion of those Protection Profiles presented scenarios challenges preventing their update towards meeting the CRA ESRs, for those specific cases it could be more convenient to explore other other routes for demonstrating conformity with CRA, such as European harmonised standards or common specifications. It must be stressed as well that at the time of publication of this report, a mutual recognition agreement that allows using protection profiles certified out of the EU under EUCC scheme does not exist.

The CRA was adopted by the Council on the 10th of October 2024, and published in the Official Journal of the EU on the 20th of November of 2024, therefore it already has entered into force at the date of release of this report. Following a period of 36 months, the Regulation will fully apply in January 2028). This timeframe provides enough anticipation for technical communities, NCCAs, etc. to analyse the gaps in the PPs they elaborate, to follow the provided guidance on mappings, and to update and re-certify the PPs.

Regarding who should be responsible for reviewing these CRA conformance claims and the related technical elements included in the EUCC the PPs (as they are now or updated in the future to meet the CRA ESRs), candidates should be in principle CRA Notified Bodies. While they might sometimes lack the necessary EUCC knowledge required to examine these materials, section **"8 EUCC CABs and conformity assessment"** studies how EUCC CABs can also meet the requirements necessary to apply to become CRA Notified Bodies. That would result in accredited entities that possess dual knowledge about EUCC and CRA, suitable to assess specific cases of CRA implementation through EUCC.

7.3. Market case of certifications without PP

Several (CC) certifications in the market have been obtained without using Protection Profiles. For certifications that don't utilize a protection profile—representing between 22-25% in recent years, according to jtsec's statistics[18] It is expected that, at some point, these products or newer versions of them will undergo certification processes under the EUCC scheme.

Manufacturers may use this opportunity to demonstrate conformance with the CRA requirements through the new EUCC certification. In the absence of Protection Profiles for specific product types under the EUCC, manufacturers will be responsible for ensuring that the new certification process includes the necessary CC technical elements to meet the CRA ESRs. If the SFRs and SARs from previous certifications are insufficient, manufacturers will need to update the Security Target to include new requirements, ensuring that the EUCC certification addresses any gaps.

[17] https://www.ipa.go.jp/security/jisec/about/cdk3vs000000248t-att/vision_statement.pdf

[18] https://www.jtsec.es/files/2022%20CC%20Statistics%20Report.pdf

For this purpose, one of the technical implementation mechanisms listed in the Annex **"ANNEX II: Options for implementation of CRA through EUCC technical elements in STs/PPs"** , should be used in order to include in the EUCC ST those SFRs and SARs that correspond with the CRA ESRs as detailed in section **5 Meeting CRA requirements through EUCC certification.** **This study recommends the following option for implementation of the required SFRs and SARs in the STs:**

- **Definition of a Protection Profile with Functional Packages** (according to section named **"Standalone Functional and assurance packages"** within the Annex "**ANNEX II: Options for implementation of CRA through EUCC technical elements in STs/PPs"**), as it is deemed as the option providing the highest balance between harmonization and flexibility.

This option would mean the elaboration of a generic protection profile for products (software, firmware, hardware) in different architectures (standalone, distributed, embedded, etc.) that contains a variety of functional packages sufficient to model the different ESRs of CRA Annex I. The SFRs related to those ESRs, along with related branches of the SPD, would be grouped together into different functional packages that could be flexibly included in or excluded in the ST in accordance with the applicability of the ESRs.

However, that option is not mandatory and manufacturers could create individual CRA-tailored STs for their products that incorporate all the EUCC technical elements that they need to meet the CRA ESRs (example, as in Annex "**ANNEX II: Options for implementation of CRA through EUCC technical elements in STs/PPs**", within the section named" **Standalone Security Target**".

7.4. Remote data processing solutions

Remote data processing solutions, when hosted in the cloud, aren't a target where EUCC can suit well for their certification (as discussed in section CC). Pending further clarifications on the notion of remote data processing solutions, the study proposes that the CRA conformance of the cloud-hosted remote processing solutions is addressed separately from the on-premise EUCC certifiable product. The conformance of the in-cloud component can be demonstrated through other assessment methods contemplated in Article 32 of CRA (e.g., based on Module H) or through application of harmonised standards.

Regardless of the condition that the scope includes remote data processing solutions or not, the remote data processing associated with the product with digital elements shall be secured, and shall comply with the ESRs of the CRA. Whether it is covered or not by the scope of the EUCC certification, or it is to be covered by other assessment procedure, it is a choice of the manufacturer. When they cannot be included in the scope of the EUCC assessment, then this assessment should include at least the verification of a secure communication link between the evaluated part of the product with digital elements included in the EUCC certification, and the remoted data processing that is not included in it.

The EUCC certification shall cover the on-premise part of the solution. Security targets and protection profiles that contemplate the certified product relying on components hosted in the cloud should include technical elements reflecting that such remote components possess an appropriate level of security assurance. This study proposes two mechanisms intended for this purpose that can be used together or individually depending on the specific certified solution:

a) The part of the solution that is EUCC-certified shall implement security measures and include in the scope of the certification, through the appropriate SFRs, the functionality for securitization of the secure channel between the on-prem and cloud components. This secure channel shall be subject of the evaluation and shall ensure the confidentiality, integrity and authenticity of the information transmitted through this channel.

b) The PP/ST should include in the Security Problem Definition the assumptions that appropriately reflect that the cloud-hosted component is trusted, e.g., by being deployed on a certified platform, being administered in a secure way by trusted administration personnel, or by having been subject of a cybersecurity certification, providing that way a level of assurance commensurate with the risk level associated to the security problem.

This solution releases manufacturers from investing efforts in attempting to include in the scope of the EUCC certification remote parts of the solution that aren't always suitable to be certified under this scheme. It also opens the door to relying on of harmonised standards for the security component or in other cybersecurity certification schemes that are more appropriate for cloud-based architectures.

In summary, the security problem definition should indicate, where applicable, the means of the remote data processing (RDP) of the product. Preferably, the RDP should be included in the scope of the product's EUCC certification, with relevant SFRs and SARs. Where the RDP cannot be included in the scope of the certification, a justification should be provided and an assumption and related operational environment requirements should be made throughout the Security Target on the security of these RDP means, that should be verified by ways of other assessment activities. At least the EUCC certificate should cover the security of the interface to the RPD.

The EUCC scheme could be supported by guidelines for the evaluation of the RDP of products under EUCC.

7.5. Addressing mismatch between EUCC and CRA scope

Many mainstream PPs and market practices for CC certifications scope only those parts of products that implement the security functions, rather than the entire product with digital elements. This limited scope can pose challenges in meeting CRA ESRs for the entire product.

A straightforward solution, such as broadening the scope of the certification to include the full scope of the product in the EUCC certification may not be suitable in all situations. Non-security components or security-related subsystems in complex systems are often not designed with security in mind and may not be hardened against threats. Including these in the cybersecurity assessment can increase the attack surface and undermine the overall security, making the certification process less effective. EUCC certification benefits most from focusing solely on security functions, as this approach simplifies, reduces costs, and speeds up evaluations.

CC offers a specific tool allowing to define different levels of security in the same certification, such as **multi-assurance** security targets (or PPs). Multi assurance, in summary, allows to specify different security regions (sub-TSF) within the same TOE, with a different set of security requirements being applicable for each region. Each security region can be assessed using different Evaluation Assurance Levels (EALs), so it is possible to define within the same evaluation different levels of security for each security region, ones more strict or critical, others being less. This mechanism could fit well with cases in which the manufacturer wishes to include the full product under the EUCC certification scope, even with those parts of it that don't implement any security function.

However, [CC2022P1] restricts the use of multi-assurance to those scenarios where a PP-configuration are used. For several mainstream PPs in the market and non-PP compliant STs, this wouldn't be an applicable option.

Another issue challenge that muti-assurance solution poses is that, at the date of publication of this study, it hasn't been adopted by the industry yet in a mainstreamed manner, as it was introduced with CC 2022. For example, no approved protection profiles or certified products using multi-assurance PP-configurations have been certified at the current date. This mechanism also couldn't be necessarily suitable for every case in the industry, an in-detail study would be required on a case-by-case basis. While multi-assurance might be a solution in the future for some products, the question that arises at this point is how compliance with the CRA can be demonstrated through EUCC, even if the certification scope is smaller than the scope of the complete product, and without using multi-assurance, as in the protection profiles that are currently on the market.

Another possible way forward would consist in applying good design principles as a means to justify that the scope of the CC TOE is adequate, even when it is smaller than the full product. **Security solutions should be developed following secure design principles ensuring that the security functions of the product protect the non-security ones.** This situation can be illustrated with the example of a certified operating system, where the certification scope covers only the kernel, security libraries, and security applications, but not the rest of the non-security applications and libraries in the user layer of the OS. For instance, the functionality that a user would use to change the appearance of their desktop, such as changing the background image or colour theme, is not a security function. Most likely, the parts of the OS architecture providing this function are outside the certified TOE scope. However, the certified security functions of the OS, in scope of the certification, shall ensure that the user personalizing their desktop has been previously authenticated and shall ensure as well that other users in the system cannot modify the background image of the first user.

The example given is a simple one but, in general, such design principles are used by certified security solutions or by certified solutions that implement security functions, as a foundation of their security. In fact, the assurance component ADV_ARC.1 Security architecture description defined in [CC2022P3], which aims to assets certain security properties of the TOE architecture, is used to assess these kind of secure design principles during EUCC evaluations.

In a similar manner, such design principles are expected to mitigate some of the risks of having less (or none) assurance in the non-certified parts of the product with respect to the certified ones. Obviously, non-security related parts of the product architecture could introduce security risks through vulnerabilities that could be present in them as a result of those parts not being target of the security assessment associated to the EUCC certification. However, **if the certified functions have been developed appropriate design security principles, it could be reasonably expected that any security weaknesses in the non-certified functions should not affect the assets protected by the evaluated security functions. For Annex I Part I ESRs, this would mean that an assumption is made that no exploitable vulnerability that might pose a risk can be found in the non-certified functions.**

Following with the previous example of the operating system presented before, the user desktop personalization function could present vulnerabilities or security weaknesses that weren't detected during the evaluation because those functions weren't included in the scope of the TOE. If the OS was developed using appropriate design principles, a vulnerability in the desktop personalisation application or library would be harmless to the assets protected by the TOE. For example, this vulnerability could not be exploited to change the desktop background or other user settings of a different user, as the protection of such settings should be in the scope of the security functions implemented in the TOE and covered by the EUCC certification.

Theoretically, during the EUCC evaluation it had been verified that such settings cannot be modified from unauthorized user software, even if this software is malicious or compromised, due to the fact that the OS parts controlling those settings were verified as free of vulnerabilities during the evaluation. If the uncertified vulnerable application were able to modify such settings, that would be a symptom that the code within the TOE implementing the security protection of the settings is not secure.

Based on the above-presented rationale, when the scope of the TOE in a EUCC certification is smaller than the scope of the CRA product with digital elements, **this study proposes that manufacturers demonstrate that the security functions included in the scope of the TOE chosen for the EUCC evaluation are sufficient to protect the non-security functions that are outside the scope of the evaluation.** In other words, it would be a demonstration that **the boundary of the TOE is sufficient to guarantee the security of the full product, even for the parts of it that are not in scope of the EUCC certification.** This demonstration should be done on the basis of the **cybersecurity risk assessment linked to the Security Problem Definition** of the EUCC evaluation.

This demonstration would proof that, for each particular case, it wouldn't be necessary to make the scope of the EUCC-certified TOE bigger in order to cover other non-EUCC-certified parts of the product with digital elements. It means that the certification of the security related functionalities would be sufficient to demonstrate that the full product meets the ERS in Part I and Part II. It will need to be further discussed to what extent such an approach would be deemed sufficient for the future presumption of conformity, given that the CRA requires conformity assessment for the full product.

In to incorporate this demonstration of sufficiency to the EUCC certification industry, authors of STs that don't claim conformance with PPs can use the template provided in the Annex to this study, section **"Annex III. Template: CRA conformance claims for EUCC certified products"**. However, in order to avoid repetition of the same rationale for this demonstration in every individual certification process, **this study encourages that the rationale for the sufficiency of TOE boundary is included future updates of the Protection Profiles in the industry** (i.e. aligned with the arguments presented in section **7.2 Harmonised CRA implementation through PP reviews and updates**).

As an alternative to the above proposal, for particular market cases, multi-assurance could be used, but only in those cases where using a PP-configuration is possible, in order to include the full product scope in the EUCC evaluation.

Finally, the analysis carried out on PPs or individual STs shall take into account that, with respect of vulnerability analysis, when AVA_VAN.2 or higher is included the evaluation, then the non-TOE parts of the product are examined in search of vulnerabilities during the AVA_VAN campaign, according to AVA_VAN.2.2E (see [CC2022P3]), as already pointed out in section 5.4 Scope of the assessment in EUCC vs CRA. In cases where AVA_VAN.1 is the highest AVA_VAN level included in the PP/ST, then the analysis proposed in the current subchapter applies.

7.6. Summary of the strategy

Based on the reasoning elements provided so far in this chapter, this subchapter proposes a possible solution to address the gaps in CC certifications in the market (and future EUCC certifications) that don't currently, according to the analysis presented in this study, possess all the necessary elements that would be required in order to meet the CRA ESRs through EUCC certifications.

The scenario starts with a manufacturer aiming to use the certificate of a product with digital elements in the market that has been EUCC-certified in order to demonstrate conformance with CRA. Under this scenario there are two fundamental cases:

a) The EUCC certification claims conformity with a protection profile.
b) The EUCC certification does not claim conformity with any protection profile.

7.6.1. Case a: EUCC certification compliant with Protection Profiles

The industry, such as the communities in charge of the elaboration and maintenance of the PPs, should provide the necessary support to avoid that manufacturers and CABs have to reanalyse in the case of any individual product whether the EUCC certification covers all the necessary technical elements required in order to meet the CRA ESRs through EUCC.

As such, this study proposes that for this case, the effort is performed as far as possible on the side the stakeholders responsible for maintaining the PPs. Then, manufacturers would reuse as much as possible of the results in the analysis done at PP-level.

Initial phase: PP assessment

The author of the PP shall use the guidance provided in this document (or in future guidance if available after the publication of this report) to determine whether the following conditions are met:

1) If the essential requirements in CRA Annex I are met by the technical elements in the EUCC certification.
    i. The PP author, on the basis of the risk analysis linked to the EUCC Security Problem Definition, shall identify which CRA ESRs of Annex I, part I are applicable for their product with digital elements. Then, it will elaborate a statement of applicability of those ESRs (e.g., using the template given in the Annex to this study, section **"Annex III. Template: CRA conformance claims for EUCC certified products"**), in which:
        a. For each CRA ESR in Annex I, part I deemed as **applicable**, it shall be indicated which technical elements in the EUCC Security Target cover that ESR between those of the mapping provided in this guidance, or by other alternative technical elements.
        b. For each CSA ESR in Annex I, Part I, deemed as **not applicable**, it shall be indicated, on the basis of and referring to the elements of the Security Problem Definition in the EUCC ST (threats, assets, assumptions, etc.) why the ESR is not applicable.
    ii. If there are remaining CRA ESRs in Annex I, Part I (deemed as applicable) **or Part II**, but aren't covered in the EUCC certification though the applicable technical elements, then **a gap in the ESR coverage is found: "GAP (ESRs)".**

2) If the scope of the product with digital elements is equal to the scope of the TOE under the EUCC certification.
    i. It shall be documented, e.g., using the template given in the Annex to this study, section **"Annex III. Template: CRA conformance claims for EUCC certified products"**, the comparison between both scopes, as follows:
        a. If both scopes are **equals**, then no further justification is needed.
        b. If the scope of the EUCC TOE is **smaller** than the scope of the product with digital elements, then it shall be justified, on the basis of the risk analysis

linked to the CC SPD, and referring to its elements, that the boundary of the TOE under scope of the EUCC certification is sufficient to protect the whole scope of the product with digital elements.

ii. If, ***i*.a** doesn't stand and in step ***i.b***, it is not possible to justify that the chosen TOE boundary brings the necessary level of protection to the whole product, then **a gap in the TOE scope is found: "GAP (scope)"**

3) If the remote data processing solutions of the product with digital elements are covered under the scope of the certification:
   i. It shall be documented, e.g., using the template given in the Annex to this study, section **"Annex III. Template: CRA conformance claims for EUCC certified products",** which remote data processing solutions are used by the product with digital elements. For each of them:
      a. If the remote data processing solution is included in the scope of the EUCC certification, it shall be indicated in the justification.
      b. If the remote data processing solution is not covered in the scope of the EUCC certification, then, it shall be indicated in the template which SFRs in the Security Target and/or assumptions in the SPD ensure a secure communication channel between the TOE and the remote data processing solution.

   ii. If, in *i.a* doesn't stand and for *i.b* there are no sufficient elements of justification, then **a gap is found with respect to the remote data processing solutions: "GAP (remote)"**

If none of the gaps mentioned above are found, the PP can be considered as being able to meet the ESRs. Then:

- The statements and justifications elaborated in the previous steps should be reviewed and validated by a CRA Notified Body and validate them.
- Once reviewed, they should be made publicly available to PP users (manufacturers of products compliant with that PP).
- Manufacturers of products that will be EUCC certified in compliance with those PPs, should demonstrate through EUCC evaluations that their products are compliant with the applicable PPs. If the product is demonstrated (through PP-compliant certification) to be compliant with a PP that could meet also the CRA ESRs, then it can be considered that the EUCC-certified product also meets with the CRA ESRs.
  - With regards to remote data processing solutions, in the documentation (as seen in **section 7.4 Remote data processing solutions**) it will be indicated for each remote data processing solution, which to harmonised standard, common specification or European cybersecurity certification schemes are applied to the remote data processing solution.
  - **Note**: If the ST of a product with digital elements compliant with the PPs present relevant changes with respect to the PPs, in terms of Security Problem Definition, ESRs, SARs, or scope of the product, then the statements and justifications of the PP should be revised and refined by the author of the ST, and provided to the CRA Notified Body for review and validation.

It must be noticed that this process **does not require any changes in the PP, but the elaboration of documentation supplementary to the PP.**

If any of the gaps mentioned above are found, then the PP should undergo an update process, and its next version should address those gaps by modifications in the content of the PP, as explained in the phase below.

Second phase: PP update

The technical communities or other stakeholders in charge of maintenance of the PPs should update those PPs under EUCC, in order to incorporate in them the technical elements required meet the CRA ESRs through EUCC, in order to fill the previously mentioned gaps. The gaps should be covered as follows.

Resolution to Gap in the ESR coverage is found: "GAP (ESRs)".

The **PP shall be updated** introducing any of the following modifications as needed:

1. Changes in the Security Problem Definition: e.g., redefining assets, threats, assumptions of the operational environment or organisational security policies in order to create a cybersecurity risk assessment that support the selection
2. Inclusion of new SFRs or modification of existing ones (e.g., refinements or iterations).
3. Inclusion of new SARs (e.g., adding new assurance activities) or modification of existing ones.

Resolution to Gap in the TOE scope is found: "GAP (scope)"

The **PP shall be updated** as follows:

1. If it's possible to make the TOE equals to the scope of the product with digital elements, i.e., it doesn't pose risks for the overall security of the solution or for the certification, then the scope can be broadened to match that of the product with digital elements.
2. Otherwise, the TOE boundary shall be reviewed in order to ensure that, while being smaller than that of the full product, in consistency with the Security Problem Definition and the SFRs and SARs, it provides an adequate level of protection to the whole scope of the product with digital elements.
    a. If needed to support steps 1 or 2, then the steps 1, 2 or 3 of the resolution o **Gap in the ESR coverage is found: "GAP (ESRs)"** into can be followed to modify the PP as needed.

Resolution to Gap with respect to remote data processing solutions: "GAP (remote)"

The **PP shall be updated** as follows, as needed**:**

1. The Security Problem Definition should be changed to include assumptions and objectives for the operational environment that establish an axiomatic trust relationship on each remote data processing solution used by the TOE, and/or threats related to the communication channels between the TOE and the remote data processing solutions. For example, the assumptions of the SPD
2. SFRs shall be added or update in order to establish secure communication channels between the TOE and the remote data processing solutions.

The above changes shall be done **taking into account the guides published** with the objective of meeting the CRA ESRs through EUCC.

After performing the previous updates, the PPs shall be EUCC - recertified and the information on the statements and justifications for CRA compliance (e.g., as in the template of the Annex to this study, section **"Annex III. Template: CRA conformance claims for EUCC certified products"**) shall be provided to the CRA notified body.

When the update of the PP addresses the **Gap with respect to remote data processing solutions: "GAP (remote)",** users of the PP (manufacturers certifying their products under EUCC in compliance with such PP) shall update the template of statements of justification and compliance of the PP to describe which harmonised standards, common specification or European cybersecurity certification schemes are applied to the remote data processing solution.

7.6.2. Case b: EUCC certification not compliant with PPs

Manufacturers of products with digital elements that are EUCC-certified without claiming compliance with Protection Profiles shall first analyse if their STs include the elements necessary for meeting the CRA ESRs through EUCC.

Specifically, they shall follow ENISA-released guidance and perform the same steps 1), 2) and 3) of **Initial phase: PP assessment**, but applying them to the EUCC ST instead of the Protection Profile. If the assessment of the ST reveals any of the aforementioned gaps, then the manufacturer should update the EUCC certification, with a new ST that addresses those gaps.

In order to ease this task on the side of manufacturers and also on CAB's sides during the EUCC assessment, manufacturers should elaborate their STs claiming conformance a CRA-tailored protection profile. This study recommends to elaborate such PP following the model described in the section named **"PP with functional packages"** within the Annex "**ANNEX II: Options for implementation of CRA through EUCC technical elements in STs/PPs**".

Alternatively, manufacturers could follow the same steps of the previous title **Second phase: PP update** but applied to the EUCC ST instead of the PP, and to elaborate the statements of compliance and justifications (i.e., as per the model given in the Annex to this study, section **"Annex III. Template: CRA conformance claims for EUCC certified products").** Then the CRA Notified bodies shall review the ST of the product with digital elements and the mentioned justification to determine if the EUCC-certified product also complies with the CRA essential security requirements.

Since the last option would require an individual per-product assessment, this study strongly discourages manufacturers from utilizing that option.

7.7. Timelines for updates of Protection Profiles

Common Criteria Protection Profiles need to be certified, with a certificate issued by a NCCA, before they can be used in CC evaluation of products with Security Targets compliant to that PP. The CC certificates issued to those PPs **do not expire**, but the technical communities in charge of their update typically maintain and recertify them periodically.

However, with the release of the 2022 version of Common Criteria, a transition period has been to decommission the use of the previous version of CC (v3.1 R5) as specified in [CC_TRANSITION], as follows:

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.

It is still to be clarified how the EUCC will align with this transition rules. At the time of release of this draft report, the EUCC Implementing Regulation is being reviewed.

The table below shows, for the most used PPs in the last 5 years, who are the groups or entities in charge of their maintenance:

Protection Profile	**PP developed and maintained by**
Protection Profile for Hardcopy Devices	Hardcopy Devices international Technical Community (iTC)
Security IC Platform Protection Profile, Version 1.0	Atmel, Infineon Technologies AG, NXP Semiconductors, Renesas Technology Europe Ltd., STMicroelectronics
Security IC Platform Protection Profile with Augmentation Packages	Inside Secure, Infineon Technologies AG, NXP Semiconductors Germany GmbH, STMicroelectronics
collaborative Protection Profile for Network Devices	Network Device international Technical Community (ND iTC)
Machine Readable Travel Document SAC (PACE V2) Supplemental Access Control, Version 1.0	Agence nationale des titres sécurisés (ANTS)
Protection Profile for Machine Readable Travel Document with 'ICAO Application', Basic Access Control, Version 1.10	Bundesamt für Sicherheit in der Informationstechnik (BSI)
Protection Profile for Application Software	National Information Assurance Partnership
Protection profiles for secure signature creation device - Part 6: Extension for device with key import and trusted communication with signature creation application	CEN/ISSS - Information Society Standardization System
Protection profiles for secure signature creation device — Part 3: Device with key import	CEN/ISSS - Information Society Standardization System
Protection profiles for secure signature creation device — Part 5: Extension for device with key generation and trusted communication with signature creation application	CEN/ISSS - Information Society Standardization System
Protection profiles for secure signature creation device — Part 4: Extension for device with key generation and trusted communication with certificate generation application	CEN/ISSS - Information Society Standardization System

Machine Readable Travel Document with ICAO Application Extended Access Control with PACE, Version 1.3	Bundesamt für Sicherheit in der Informationstechnik (BSI)
Machine Readable Travel Document using Standard Inspection Procedure with PACE (PACE_PP)	Bundesamt für Sicherheit in der Informationstechnik (BSI)
Protection Profile for Mobile Device Fundamentals Version 3.3	Mobile Technical Community
Protection Profile for Mobile Device Fundamentals, Version 3.1	Mobile Technical Community
Digital Tachograph - Vehicle Unit (VU PP) Version 1.15	Joint Research Centre of the European Commission
Digital Tachograph - External GNSS Facility (EGF PP)	Joint Research Centre of the European Commission
Digital Tachograph - Tachograph Card	Joint Research Centre of the European Commission
Digital Tachograph - External GNSS Facility	Joint Research Centre of the European Commission
Digital Tachograph - Motion Sensor	Joint Research Centre of the European Commission
Digital Tachograph - Vehicle Unit	Joint Research Centre of the European Commission
Digital Tachograph - Vehicle Unit (VU PP) Version 1.0	Joint Research Centre of the European Commission
Common Criteria Schutzprofil (Protection Profile) Schutzprofil 1: Anforderungen an den Netzkonnektor	Federal Office for Information Security
Common Criteria Schutzprofilfur Basissatz von Sicherheitsanforderungen an Online-Wahlprodukte, Version 1.0	Gesellschaft für Informatik e. V.
Protection Profile for General Purpose Operating Systems Version 4.3	National Information Assurance Partnership
collaborative Protection Profile for Full Drive 2 Encryption - Encryption Engine	Full Drive Encryption 3 international Technical Community
Protection profiles for TSP Cryptographic modules - Part 5- Cryptographic Module for Trust Services (prEN 419 221-5, version 0.15)	Technical Committee CEN/TC 224 WG17
Peripheral Sharing Switch (PSS) for Human Interface Devices Protection Profile	Information Assurance Directorate (IAD)
Digital Tachograph - Smart Card (Tachograph Card)	Joint Research Centre of the European Commission
PP-Module for Stateful Traffic Filter Firewalls	Network international Technical Community
collaborative Protection Profile for Stateful Traffic Filter Firewalls	Network international Technical Community
Enterprise Security Management - Policy Management Version 2.1	ESM Protection Profile Technical Community
Korean National Protection Profile for Single Sign On V1.0	National Security Research Institute (NSR) and Telecommunications Technology Association (TTA)
Korean National Protection Profile for Single Sign On V1.1	National Security Research Institute (NSR)

Operating System Protection Profile, Version 2.0	atsec, German Federal Office for Information Security (BSI)
Digital Tachograph - Motion Sensor	European Commission - Joint Research Centre
PP-Configuration Mobile Device Management – Trusted Server (MDM-TS) complemented with PP-Module Trusted Communication Channel (TCC)	Deutsches Forschungszentrum für Künstliche Intelligenz GmbH DFKI // Bundesamt für Sicherheit in der Informationstechnik BSI)
Protection Profile Mobile Device Management – Trusted Server (MDM-TS)	Deutsches Forschungszentrum für Künstliche Intelligenz GmbH DFKI // Bundesamt für Sicherheit in der Informationstechnik BSI)
Common Criteria Protection Profile Mobile Card Terminal for the German Healthcare System (MobCT)	Federal Office for Information Security
Fingerprint Spoof Detection Protection Profile based on Organisational Security Policies (FSDPP_OSP), Version 1.7	German Federal Office for Information Security (BSI)
ePassport Protection Profile V2.1, Version 2.1	KISA Korea Internet & Security Agency
Common Criteria Protection Profile for Inspection Systems, Version 1.01	Bundesamt für Sicherheit in der Informationstechnik
DCSSI-PP-2008/04 On-the-fly Mass Storage Encryption Application (CC3.1), Version 1.4	Trusted Labs S.A.S., DCSSI
PP-Module for Wireless Local Area Network (WLAN) Client Version 1.0	NIAP
PP-Module for Wireless Local Area Network (WLAN) Access System Version 1.0	NIAP
Extended Package (EP) Wireless Local Area Network (WLAN) Clients	NIAP
Java Card Protection Profile - Open Configuration	Oracle Corporation
Java Card System – Closed Configuration Protection Profile Version 3.1, June 2020	Oracle Corporation
Protection Profile for Secure Signature Creation Device	Technical Committee CEN/TC 224
Korean National Protection Profile for Electronic Document Encryption V1.0	National Security Research Institute (NSR)
Korean National Protection Profile for Electronic Document Encryption V1.1	National Security Research Institute (NSR)
Korean National Protection Profile for Electronic Document Encryption V3.0	National Security Research Institute (NSR)
Protection Profile PC Client Specific Trusted Platform Module Specification Family 2.0; Level 0; Revision 1.59 Version 1.3	Trusted Computing Group
PC Client Specific Trusted Platform Module Family 1.2; Level 2, Version 1.1	Trusted Computing Group
PC Client Specific Trusted Platform Module Family 1.2; Level 2, Version 1.1	Trusted Computing Group
PC Client Specific Trusted Platform Module (Family 2.0, Level 0, Revision 1.16, Version 1.0)	Trusted Computing Group

(U)SIM Java Card Platform Protection Profile / Basic Configuration (ref. PU-2009-RT-79, version 2.0.2), Version 2.0.2	Société Française du Radiotéléphone (SFR)
U)SIM Java Card Platform Protection Profile Basic and SCWS Configurations, Version 2.0.2	Société Française du Radiotéléphone (SFR)
Extended Package for Mobile Device Management Agents	NIAP
Protection Profile for Application Firmware of Secure Smartcard Reader for Electronic Identity Verification System	National Research Center of Electronics and Cryptography
IEEE Standard Protection Profile for Hardcopy Devices in IEEE Std 2600-2008, Operational Environment B	Information Assurance Committee of the IEEE Computer Society
Protection Profile - Secure Signature-Creation Device Type 1, Version 1.05	CEN/ISSS – Information Society Standardization System, Workshop on Electronic Signatures
Protection Profile Configuration for Network Device and SSL/TLS Inspection Proxy	atsec, NIAP
NDhPP PP for Network Device Management (NDhPP), version 1.0, 2021-04-23	(FORBIDDEN)
Protection Profile for IPsec Virtual Private Network (VPN) Clients	NIAP
Intrusion Detection System Scanner Protection Profile	Science Applications International Corporation
PP-Module for Stateful Traffic Filter Firewalls	Network international Technical Community
Protection Profile for Database Management Systems (DBMS PP) Base Package	DBMS Working Group Technical Community
Electronic Identity Card (ID_Card PP), Version 1.03	Bundesamt für Sicherheit in der Informationstechnik
Smartcard IC Platform Protection Profile	Atmel Smart Card ICs, Hitachi Europe Ltd., Infineon Technologies AG, Philips Semiconductors
Intrusion Detection System System Protection Profile	Science Applications International Corporation
collaborative Protection Profile for Stateful Traffic Filter Firewalls	Network international Technical Community
Protection Profile for Enterprise Security Management Access Control	NIAP
New Generation Cash Register Fiscal Application Software Protection Profile 2	Revenue Administration Department / Gelir İdaresi Başkanlığı
New Generation Cash Register Fiscal Application Software Protection Profile	Revenue Administration Department / Gelir İdaresi Başkanlığı
Application-level Firewall Protection Profile for Basic Robustness Environments	National Institute of Standards and Technology, National Security Agency
JavaCard System Standard 2.2 Configuration Protection Profile, Version 1.0b	Trusted Logic SA, Sun Microsystems
BSI-CC-PP-0117-V2-2023 Secure Sub-System in System-on-Chip (3S in SoC), Version 1.8	Eurosmart

Embedded UICC for Consumer Devices, Protection Profile, Version 1.0 05-June-2018	GSM Association
ETSI TS 103 732-1 V2.1.2 (2023-11) CYBER; Consumer Mobile Device; Part 1: Base Protection Profile	ETSI
ETSI GS QKD 016 V2.1.1 (2024-01) Quantum Key Distribution (QKD); Common Criteria Protection Profile - Pair of Prepare and Measure Quantum Key Distribution Modules	ETSI
Protection Profile for Smart Meter Minimum Security requirements, Version: 1.0, Date: 30. October 2019	ESMIG

Table 11 Protection Profiles and their developers

This study recommends the entities in charge of updating the PPs to use the opportunity of the necessary update on the deadline established for the adaptation to CC2022 for also ensuring that the PPs are updated to be compliant with CRA.

Moreover, at the light of the analysis conducted in section **"6 Analysis of the EUCC certification landscape for Critical and Important products"**, when it comes to implementation of CRA through PP-compliant EUCC certifications the gap in the PPs used to certify critical products with digital elements listed in CRA Annex IV in general, smaller than that in the PPs used to certify critical products with digital elements listed in CRA Annex III. Therefore, the industry might consider more convenient to prioritize the review and adaptation process of those PPs used in the industry for the EUCC certification of critical products.

8. EUCC CABs and conformity assessment

Under the CSA, competent CABs have to undergo accreditation and (only for assurance level high) authorisation in line with Article 61. Furthermore, the accredited or authorised CABs have to be notified by Member States to the Commission.

This section aims to provide a high-level analysis of how the EUCC CABs could meet the requirements applicable to CRA Notified Bodies. For example, EUCC accreditation requirements are more specific than the ones that apply to CRA Notified Bodies. Anyway, the value of this analysis resides in the possibility of having EUCC CABs that are also CRA Notified Bodies, as they could be potential candidates to assess aspects related to the interplay between EUCC and CRA, for example, if an CC PP has been properly updated under EUCC scheme in order to comply with the CRA ESRs.

In the case of CRA, in order to be notified as a CAB under CRA, an accreditation process is not required as a prerequisite, but the CABs in order to be eligible for notification need to meet and prove to the notifying authority the requirements listed in Article 39 of CRA.

The table presented below provides a detailed analysis of how each requirement in Article 39 of CRA can be met by the EUCC CAB requirements described in the Annex of the CSA. This analysis is made without considering further specifications that might be done of the CAB requirements under the EUCC.

For information purposes, links to related requirements from ISO/IEC 17065 that may support compliance of the indicated CRA requirements for CABs are provided in the last column of the table. ISO/IEC 17021 requirements related to Module H have not been analysed, as the assessment methods associated to EUCC certification processes resemble more to the third-party assessments carried out when CRA conformance is demonstrated through the EU-type examination procedure (based on module B) followed by conformity to EU-type based on internal production control (based on module C).

The analysis detailed in the table below shows that the CSA requirements are similar to the requirements for CRA Notified Bodies set out in CRA Article 39, pending further specifications under respective frameworks. This might suggest that CABs could be notified both under EUCC and CRA.

Article 39 paragraph / CRA CAB requirement for notification		Coverage by CSA Annex [EUCC]	Analysis	Obs./ Gaps	Supporting ISO/IEC 17065 requirement
1	For the purposes of notification, a conformity assessment body shall meet the requirements laid down in paragraphs 2 to 12.	N/A	Analysis provided for paragraphs 2-12 below.	N/A	
2	A conformity assessment body shall be established under national law and have legal personality.	Covered: CSA Annex, paragraph 1	Direct correspondence	N/A	ISO/IEC 17065, 4.1.1

3	A conformity assessment body shall be a third-party body independent of the organisation or the product with digital elements it assesses.	Covered: CSA Annex, paragraph 2 CSA Annex, paragraph 3	Direct correspondence	N/A	ISO/IEC 17065, 4.2.2
4	A conformity assessment body, its top-level management and the personnel responsible for carrying out the conformity assessment tasks shall not be the designer, developer, manufacturer, supplier, importer, distributor, installer, purchaser, owner, user or maintainer of the products with digital elements which they assess, nor the authorised representative of any of those parties. This shall not preclude the use of assessed products that are necessary for the operations of the conformity assessment body or the use of such products for personal purposes.	Covered: CSA Annex, paragraphs 4, 5, 6, 7	Direct correspondence	N/A	ISO/IEC 17065, 4.2.6 [Impartiality]
5	Conformity assessment bodies and their personnel shall carry out the conformity assessment activities with the highest degree of professional integrity and the requisite technical competence in the specific field and shall be free from all pressures and inducements, particularly financial, which might influence their judgement or the results of their conformity assessment activities, especially as	CSA Annex, paragraph 8	Direct correspondence	N/A	ISO/IEC 17065, 4.2.8 Impartiality

	regards persons or groups of persons with an interest in the results of those activities.				
6.a	A conformity assessment body shall be capable of carrying out all the conformity assessment tasks referred to in Annex VI and in relation to which it has been notified, regardless of whether those tasks are carried out by the conformity assessment body itself or on its behalf and under its responsibility. At all times and for each conformity assessment procedure and each kind or category of products with digital elements in relation to which it has been notified, a conformity assessment body shall have at its disposal the necessary: a) personnel with technical knowledge and sufficient and appropriate experience to perform the conformity assessment tasks;	Covered: CSA Annex, paragraphs 10,11	Direct correspondence	N/A	ISO/IEC 17065, 6.1.1
6.b	descriptions of procedures in accordance with which conformity assessment is to be carried out, ensuring the transparency and the ability of reproduction of those procedures. It shall have appropriate policies and procedures in place	Covered: CSA Annex, paragraphs 10, 11	Direct correspondence	N/A	ISO/IEC 17065, 7.1.1

	that distinguish between tasks it carries out as a notified body and other activities;				
6.c	procedures for the performance of activities which take due account of the size of an undertaking, the sector in which it operates, its structure, the degree of complexity of the product technology in question and the mass or serial nature of the production process.	Covered: CSA Annex, paragraphs 10, 11	Direct correspondence	N/A	ISO/IEC 17065, 7.1.1
7.a	A conformity assessment body shall have the means necessary to perform the technical and administrative tasks connected with the conformity assessment activities in an appropriate manner and shall have access to all necessary equipment or facilities. The personnel responsible for carrying out conformity assessment activities shall have the following: (a) sound technical and vocational training covering all the conformity assessment activities in relation to which the conformity assessment body has been notified;	Covered: CSA Annex, paragraph 12	Direct correspondence	N/A	ISO/IEC 17065, 6.1.2 Competence
7.b	satisfactory knowledge of the requirements of the assessments they carry out and adequate authority to carry out those assessments;	Covered: CSA Annex, paragraph 12	Direct correspondence	N/A	ISO/IEC 17065, 6.1.2 Competence
7.c	appropriate knowledge and understanding of the essential requirements,	Covered: CSA Annex, paragraph 12	Direct correspondence	N/A	ISO/IEC 17065, 6.1.2 Competence

	of the applicable harmonised standards and of the relevant provisions of Union harmonisation legislation and of its implementing acts;				
7.d	the ability to draw up certificates, records and reports demonstrating that assessments have been carried out.	Covered: CSA Annex, paragraph 12	Direct correspondence	N/A	ISO/IEC 17065, 6.1.2 Competence
8	The impartiality of the conformity assessment bodies, their top-level management and of the assessment personnel shall be guaranteed. The remuneration of the top-level management and assessment personnel of a conformity assessment body shall not depend on the number of assessments carried out or on the results of those assessments.	Covered: CSA Annex, paragraphs 13, 14	Direct correspondence	N/A	ISO/IEC 17065, 4.2.5 ISO/IEC 17065, 4.2.12 Impartiality
9	Conformity assessment bodies shall take out liability insurance unless liability is assumed by their Member States in accordance with national law, or the Member State itself is directly responsible for the conformity assessment.	Covered: CSA Annex, paragraph 15	Direct correspondence	N/A	ISO/IEC 17065, 4.3.1
10	The personnel of a conformity assessment body shall observe professional secrecy with regard to all information obtained in carrying out their tasks under Annex VI or any provision of national law giving effect to it, except in relation to the market surveillance authorities of the Member State in which	Covered: CSA Annex, paragraphs 16, 17	Direct correspondence	N/A	ISO/IEC 17065, 4.5 Confidentiality

	its activities are carried out. Proprietary rights shall be protected. The conformity assessment body shall have documented procedures ensuring compliance with this paragraph.				
11	Conformity assessment bodies shall participate in, or ensure that their assessment personnel are informed of, the relevant standardisation activities and the activities of the notified body coordination group established under Article 40 and apply as general guidance the administrative decisions and documents produced as a result of the work of that group.	Partly covered: CSA Annex, paragraph 12	The part of the paragraph 11 of CRA referring to knowledge and training requirements for personnel in CSA notified bodies is covered by the requirements for CABs personnel in paragraph 12 of CSA Annex. However, the part of the requirement related to keep personnel of notified bodies of relevant standardisation activities can’t be considered as directly covered, although there is some level of relation between both paragraphs.		ISO/IEC 17065, 6.1.2 Competence
12	Conformity assessment bodies shall operate in accordance with a set of consistent, fair, proportionate and reasonable terms and conditions, while avoiding unnecessary burden for economic	Covered: CSA Annex	Direct correspondence	N/A	ISO/IEC 17065, 4.2.2

	operators, in particular taking into account the interests of microenterprises and small and medium-sized enterprises in relation to fees.				

Table 12: CRA Article 39 requirements vs CSA

9. Conclusions of the study

This study has analysed the possible interplays between CRA and EUCC in order to be able to meet the CRA essential security requirements through EUCC certificates. In other words, if a product on the market that has obtained an EUCC certificate after undergoing a security evaluation through an EUCC CAB can be assumed as possessing the necessary security assurance and coverage that is required to comply also with the essential security requirements (ESRs) of the CRA. Since at the date of release of this report no EUCC certificates have been issued, these conclusions refer to future EUCC certifications.

A mapping between those ESRs and technical elements in CC (e.g., Security Functional Requirements and Security Assurance Requirements) evidences the extent to which CRA ESRs can be met by future EUCC certifications. This study elaborates on a proposal of those mappings; however, the proposal is not the only one that could be valid for this purpose and manufacturers could justify the compliance with CRA ESRs through different sets of CC technical elements or other ways allowed at the CRA.

At the same time, the risk assessment linked to the CC Security Problem Definition is an effective tool for manufacturers to justify the applicability or non-applicability of the CRA ESRs in Annex I Part I, which would result in the inclusion of certain CC technical elements in the certification, while others would be left out.

The study has showed that meeting the CRA through EUCC will not only involve meeting the essential security requirements of CRA Annex I, but it also requires that the scope of the TOE in the EUCC certification will correspond to that of the product with digital elements placed on the internal market, including the remote data processing solutions that are required by the product for its correct functioning. These requirements had been addressed in the study and proposals are presented.

The analysis carried out in this document stresses that the solutions based on technical elements, should take into account the reality of the current CC certification industry, and therefore invites stakeholders to feed back their experience.

This industry largely functions based on protection profiles, especially in the case of products that fall under the Critical Products of Annex IV and the Important products of Annex III of CRA. In this regard several conclusions can be drawn. First of all, PPs define specific security scenarios and thread modelling, with specialized security solutions to be implemented uniformly by multiple products in the market when they fall under the same technological category. Protection Profiles define a baseline of security requirements. While no existing PPs seems to meet all the essential security requirements in Annex I of CRA in every individual market case, a first analysis seems to suggest that the gap is narrower for existing PPs covering critical products than for important products. However, a more exhaustive analysis would be required in particular for important products.

Moreover, Protection Profiles also define the scope of the EUCC certification. Several of the mainstream PPs in the industry define a certification scope that is smaller than the scope of the product with digital elements. In this regard, the study suggests that it could be demonstrated that the certification of security related functionalities is sufficient to ensure the security of the whole product. However, this might not be possible for all products.

In particular, the remote data processing solutions is part of the products have to be included in the scope according to the CRA and meet the ESRs. Remote data processing, pending further clarification of the concept, are not in the scope of the EUCC assessment in the majority of the PPs currently in the market. In some PPs, secure communication is covered, however it is not expected to be sufficient. In this case, the study stressed that the current version of CC standard that will be used under EUCC scheme is not suitable for the nature of cloud-based solutions and therefore manufacturers might explore other certification strategies.

Protection Profiles highly condition the degree of interoperability of existing CC and future EUCC certification approaches, and therefore modify them in order to add CC technical elements or to modify the scope of the assessment needs to be considered by considering the whole ecosystem. Based on these reasons, this study proposes different possible way forward. First of all, it might be possible, based on justifying, on the basis of risk assessment and Security Problem Definition in CC that the existing EUCC PP-based certificates in the market already provide a coverage of security functions that is sufficient for their intended usage in their expected deployment environment, regardless of the fact that some ESRs of the CRA aren't covered. This however means that the risk assessment should conclude that the covered CRA ESRs (in Annex I Part 1) are not necessary. The existing PP-based certifications should also demonstrate that the boundary of the EUCC certification is sufficient to ensure that the security functions under the scope of the certification are sufficient to protect the security of the whole product, even of the non-certified parts.

With regards to remote data processing solutions, there may be cases where EUCC would not offer suitable ways to assess their compliance with CRA. In order to determine if that would be the case, the Security Problem Definition should indicate, where applicable, the means of the remote data processing (RDP) of the product. Preferably, the RDP should be within the scope of the product's EUCC certification, including relevant SFRs and SARs. If this is not feasible, a justification should be provided, along with assumptions and operational environment requirements in the Security Target regarding the security of the RDP, verified through other assessment activities. At a minimum, the EUCC certificate should address the security of the interface to the RDP. Guidelines for evaluating the RDP under the EUCC scheme could further support this process.

In the case of those Protection Profiles presenting gaps in the compliance with CRA that cannot be duly justified (i.e., through risk assessment demonstrating that certain ESRs aren't applicable or justification that the TOE boundary is sufficient to protect the non-TOE parts of the product), it will be required an update of the PP. This study proposes that, in a second stage, those PPs are updated in order to include in them those CC technical elements required to fill the gaps in their compliance with CRA requirements, for example, by adding new SFRs or SARs.

In order to do both the demonstration of compliance and the update of the PPs, guidance should be provided for manufacturers and PP authors. This study proposes several technical inputs that could be used as a basis for such tasks.

In the remaining share of the certification industry that doesn't rely on PPs, this study also proposes the elaboration of either guidance or Protection Profiles that, in a generalist manner, can be used in any type of product so as to incorporate the EUCC elements necessary to meet the CRA essential security requirements in a harmonized way.

The study has also analysed and demonstrated that the EUCC CABs will notionally meet, at level high, the requirements that Article 39 of CRA imposes for Notified Bodies, therefore they have the necessary competence to perform assessment of conformance with CRA. Nonetheless, in order for them to be able to assess aspects related to CRA implementation through EUCC, they should be trained on CRA-specific technical aspects. Entities qualifying as both CRA Notified Bodies and EUCC CABs would be suitable candidates to assess whether future updates in EUCC PPs are sufficient to meet the CRA ESRs.