UNIVERSITY OF PERAEUS

SCHOOL OF INFORMATION AND COMMUNICATION TECHNOLOGIES
DEPARTMENT OF DIGITAL SYSTEMS

MSc DIGITAL SYSTEMS SECURITY

MASTER’S DISSERTATION PROJECT

EU Cybersecurity Certification Scheme on Common Criteria (EUCC)

Maristela Chairetaki

Supervisor Professor:
Konstantinos Lambrinoudakis

PIRAEUS

FEBRUARY 2025

MASTER’S DISSERTATION PROJECT

EU Cybersecurity Certification Scheme on Common Criteria (EUCC)

Maristela Chairetaki
A.M.: MTE2228

ΠΕΡΙΛΗΨΗ

Η ακόλουθη διπλωματική εργασία αποτελεί το τελικό σκέλος των μεταπτυχιακών σπουδών στο πλαίσιο του προγράμματος «Ασφάλεια Ψηφιακών Συστημάτων» του Τμήματος «Ψηφιακών Συστημάτων» του Πανεπιστημίου Πειραιώς. Το επιλεγμένο θέμα για αυτή τη διατριβή περιλαμβάνει το σχήμα του EUCC, ενός πρόσφατα προσαρμοσμένου προτύπου πιστοποίησης κυβερνοασφάλειας της ΕΕ, το οποίο δημιουργήθηκε μετά από πρωτοβουλία του νόμου της ΕΕ για την κυβερνοασφάλεια (EU Cybersecurity Act). Το Σύστημα Πιστοποίησης Κυβερνοασφάλειας της Ευρωπαϊκής Ένωσης με κοινά κριτήρια (EUCC) αντιπροσωπεύει μια σημαντική πρωτοβουλία που στοχεύει στην ενίσχυση της ασφάλειας των προϊόντων Τεχνολογίας Πληροφορικής και Επικοινωνιών (ΤΠΕ) σε ολόκληρη την ΕΕ. Αυτή η διατριβή εξετάζει το νομικό πλαίσιο, τους στόχους, τις προκλήσεις εφαρμογής και την ευθυγράμμιση του EUCC με τα διεθνή πρότυπα κυβερνοασφάλειας. Αναλύοντας τις αρχές των κοινών κριτηρίων και την εφαρμογή τους στο EUCC, η μελέτη υπογραμμίζει τον ρόλο του συστήματος στη διασφάλιση της εμπιστοσύνης και της συμμόρφωσης μεταξύ των ενδιαφερομένων. Επιπλέον, η έρευνα διερευνά τον αντίκτυπο του EUCC στην ψηφιακή αγορά, τις προκλήσεις υιοθέτησής του και πιθανές μελλοντικές εξελίξεις. Τα ευρήματα υπογραμμίζουν τη σημασία μιας εναρμονισμένης προσέγγισης πιστοποίησης για την ενίσχυση του τοπίου της κυβερνοασφάλειας της ΕΕ.

ΘΕΜΑΤΙΚΗ ΠΕΡΙΟΧΗ: Πρότυπο πιστοποίησης κυβερνοασφάλειας της ΕΕ

ΛΕΞΕΙΣ ΚΛΕΙΔΙΑ: Πρότυπο πιστοποίηση κυβερνοασφάλειας, EU Cybersecurity Act, Common Criteria, Ασφάλεια ΤΠΕ, ENISA

ABSTRACT

The following thesis constitutes the final segment of postgraduate studies within the framework of the “Digital System Security” program of the Department of “Digital Systems” at the University of Piraeus. The chosen topic for this thesis involves the context of EUCC, a newly adapted EU cybersecurity certification standard, that has been created after the initiative from the EU Cybersecurity Act. The European Union Cybersecurity Certification Scheme on Common Criteria (EUCC) represents a significant initiative aimed at enhancing the security of Information and Communication Technology (ICT) products across the EU. This thesis examines the EUCC's legal framework, objectives, implementation challenges, and alignment with international cybersecurity standards. By analyzing the Common Criteria principles and their application within the EUCC, the study highlights the scheme’s role in ensuring trust and compliance among stakeholders. Furthermore, the research explores the impact of the EUCC on the digital market, its adoption challenges, and potential future developments. The findings underscore the importance of a harmonized certification approach to strengthen the EU’s cybersecurity landscape.

SUBJECT AREA: EU Cybersecurity certification standard

KEYWORDS: Cybersecurity certification standard, EU Cybersecurity Act, Common Criteria, ICT Security, ENISA

ACKNOWLEDGMENTS

For the successful completion of this thesis, I would like to express my heartfelt gratitude to my advisor, Professor Panagiotis Rizomiliotis, for his invaluable guidance, continuous support, and expert insights throughout this academic journey. His dedication and encouragement have played a crucial role in shaping the outcome of this work.

I also, wish to express my deepest gratitude to my parents and loved ones, who have been my pillars of strength and support throughout this journey. Their unwavering belief in me, encouragement, and endless patience have given me the motivation to persevere and strive for excellence in all my endeavors.

Lastly, a special thanks goes to my beloved cousin Michalis, who, although no longer with us, had been a source of comfort and guidance. His support and faith in my potential remains etched in my heart forever. This work is a tribute to the special bond we shared and especially the encouragement he gave me during my studies. A special thanks also goes to his wife and kids, whose strength and love have been a constant reminder of the values he has conveyed in all of us.

TABLE OF CONTENTS

LIST OF TABLES

1. INTRODUCTION

With the increasing dependance on digital infrastructure, cybersecurity has become a critical concern for governments, businesses, and individuals. As cyber threats continue to evolve in sophistication and scale, ensuring the security and resilience of Information and Communication Technology (ICT) products is more critical than ever. One of the most effective ways to achieve this is through the establishment of an up-to-date cybersecurity certification, which will provide a standardized and structured approach to evaluating and validating security measures. Certification frameworks help establish trust among users, regulatory bodies, and industry stakeholders by ensuring compliance with rigorous security standards.

The European Union throughout the years has actively pursued regulatory measures, responding to these concerns through various regulatory frameworks, with the EU Cybersecurity Act serving as a cornerstone of these efforts. Among the key initiatives under the Cybersecurity Act is the EU Cybersecurity Certification Scheme on Common Criteria also known as EUCC, which aims to provide a unified, recognized framework for the assessment and certification of ICT products within the EU. As the title of the certification suggests, the EUCC is built upon the Common Criteria (CC) framework, a globally accepted standard for evaluating the security properties of IT products and systems.

This thesis provides a comprehensive analysis of the EUCC, examining its objectives, legal foundation, and implementation strategy. It explores the role of Common Criteria in enhancing the security assurance of ICT products and examines the involvement of key stakeholders, including ENISA, certification bodies, national authorities, and industry players, in shaping and maintaining the certification landscape. Additionally, the study highlights the importance of the Common Evaluation Methodology (CEM), which standardizes the evaluation process by defining specific assurance levels and assessment procedures, ensuring consistency and reliability in cybersecurity certification.

To provide a broader context, this study also discusses the EUCC's alignment with international standards and its role in facilitating mutual recognition agreements. Finally, the research highlights the challenges associated with EUCC adoption and explores potential improvements to enhance its effectiveness in a rapidly evolving cybersecurity landscape.

This thesis is structured as follows. The first chapter introduces the concept of cybersecurity certification and provides an overview of its significance. The second chapter delves into the European Union's cybersecurity certification framework, explaining the objectives and impact of the EUCC. The third chapter presents an in-depth examination of the Common Criteria framework, including its key components and evaluation methodologies. The fourth chapter discusses the certification process under the EUCC, outlining the roles of stakeholders and compliance requirements. Finally, the fifth chapter concludes the study with key findings and recommendations for the future of cybersecurity certification in the EU.

By structuring the thesis in this manner, the study aims to provide a thorough understanding of the EUCC and its implications for the broader cybersecurity landscape.

2. EUROPEAN UNION CYBERSECURITY CERTIFICATION

The European Common Criteria-based cybersecurity certification scheme (EUCC) represents a significant advancement in the realm of cybersecurity within the European Union. The EUCC was established to harmonize and enhance the evaluation and certification of Information and Communication Technology (ICT) products, including their documentation. The EUCC also provides a unified framework that aligns with international standards, as it is based on the Common Criteria. By fostering consistency across European Union member states, the EUCC facilitates unanimous recognition of the certifications and strengthens the security assurance of ICT products. This initiative supports the development of a Digital Single Market, promotes best practices in cybersecurity, and ensures compliance with relevant EU regulations, ultimately enhancing trust and confidence among users and stakeholders in the digital economy.

2.1 The Objectives and Impact of EUCC

The EUCC was created to address several key objectives related to cybersecurity and the evaluation of ICT products within the European Union:

1) **Harmonization of Certification**: The EUCC aims to harmonize the cybersecurity certification processes across EU member states. By providing a unified framework, it reduces discrepancies in national certification schemes, facilitating mutual recognition of certifications and enhancing the overall efficiency of the certification process.
2) **Enhancing Security Assurance**: The EUCC is designed to improve the security assurance of ICT products by establishing clear and consistent evaluation criteria based on the Common Criteria. This ensures that products meet specific security requirements, thereby increasing trust among users and stakeholders regarding the security of these products. This is very important as due to increasingly complex threat landscape.
3) **Support for the Digital Single Market**: The creation of the EUCC supports the development of a Digital Single Market within the EU by providing a reliable and recognized certification framework. This encourages the adoption of secure ICT products across borders, promoting trade and innovation within the digital economy.
4) **Alignment with International Standards**: The EUCC builds on established international standards, such as the Common Criteria and the Common Evaluation Methodology. This alignment ensures that the EU's certification processes are consistent with global best practices, facilitating international cooperation and recognition of certifications.
5) **Regulatory Compliance**: The EUCC helps organizations comply with relevant EU regulations and directives related to cybersecurity, such as the Cybersecurity Act. This compliance is essential for ensuring that products meet the necessary security standards required for market access within the EU.
6) **Promotion of Best Practices**: The EUCC encourages the adoption of best practices in cybersecurity evaluation and certification, fostering a culture of security within the ICT industry. This is achieved through the establishment of technical domains and state-of-the-art documents that guide the evaluation process.

2.2 Legal Framework

The European Common Criteria-based cybersecurity certification scheme (EUCC) has been officially published. The relevant regulation, known as the Commission Implementing Regulation (EU) 2024/482, was formally adopted on January 31, 2024 and was published on February 7, 2024 in the Official Journal of the European Union, making it accessible to the public. The initiative for the EUCC was driven by the European Commission, which sought to establish a coherent framework for cybersecurity certification in response to the increasing cybersecurity threats and the need for harmonization across EU member states. This effort aligns with the objectives set out in Regulation (EU) 2019/881, also known as the Cybersecurity Act, which emphasizes the importance of cybersecurity certification for ICT products. ENISA, the European Union Agency for Cybersecurity, was instrumental in supporting the development of the EUCC by providing technical expertise and guidance to ensure its alignment with international standards and best practices.

Since the EUCC was established through a regulation, it is a binding legislative act that must be applied in its entirety across all EU member states without the need for national legislation. Meaning that the rules and obligations set forth in the regulation are directly applicable and enforceable in all EU member states, ensuring a consistent approach to cybersecurity certification across the EU.

2.2.1 ENISA’s Contribution

The European Union Agency for Cybersecurity (ENISA) plays a vital role in managing and sustaining the EU’s cybersecurity certification framework under the EU Cybersecurity Act. ENISA provides technical expertise and guidance to national cybersecurity authorities and certification bodies, developing up-to-date documents, guidelines, and best practices to ensure consistent evaluation methods across member states. This keeps the certification process aligned with the latest cybersecurity threats and trends.

In addition to offering technical guidance, ENISA fosters collaboration between member states, certification bodies, and other stakeholders. By promoting information sharing and coordination, it helps create a unified approach to cybersecurity certification across Europe. The agency also maintains a central database of certified protection profiles, ensuring that certification information is publicly accessible. This includes publishing lists of certified ICT products, their status, and updates on vulnerabilities or compliance, building trust among consumers and businesses. ENISA supports the continuous improvement of the certification process by collecting data and feedback from certification activities. This helps identify trends, gaps, and areas needing refinement, ensuring the framework evolves to meet new challenges. The agency also assists in negotiating mutual recognition agreements with non-EU countries, allowing EU-certified products to be accepted globally and promoting international cooperation in cybersecurity.

Furthermore, ENISA strengthens the capabilities of national authorities and stakeholders through training programs, workshops, and resources. This capacity-building ensures all parties are well-equipped to tackle evolving cybersecurity threats. Through these multifaceted roles, ENISA not only supports the initial implementation of the certification framework but also ensures its ongoing effectiveness and adaptability in the face of future cybersecurity challenges.

2.2.2 Implementation Timeline

The development of the EUCC scheme began with a draft published on July 1st, 2020, at the request of the European Commission. This initial draft laid the foundation for what would later become the finalized EUCC regulation in 2024. For the preparation of the EUCC draft scheme to be possible, ENISA put together an Ad Hoc Working Group (AHWG) that was launched on November 27th, 2019. This group consisted of selected members, including industry representatives (such as developers and evaluators), accreditation bodies, and participants from EU member states.

The primary goal of the scheme is to establish a unified framework used among European Union countries and cover the certification of ICT Targets of Evaluation (TOE). At the time of publishing, it was named "a candidate cybersecurity certification scheme to serve as a successor to the existing SOG-IS". The EUCC was thought from the beginning to serve as the successor of the SOG-IS MRA (Senior Officials Group Information Systems Security Mutual Recognition Agreement). After the finalization and publication of the EUCC scheme, the certification process could be improved and streamlined in such a way as to provide a simplified certification process across the member states of the EU. With this new scheme addition, it was expected to eliminate inconsistencies and increase efficiency.

Beyond serving as a successor to the SOG-IS MRA, the EUCC draft aimed to enhance the cybersecurity of ICT Targets of Evaluation (TOE), particularly those incorporating security features such as encryption mechanisms and electronic signature tools. By establishing a unified and accessible certification framework, the scheme sought to protect sensitive assets, ensure the integrity of digital services, and bolster the EU’s overall cybersecurity resilience. Additionally, harmonizing certification standards across the internal market would foster trust among stakeholders while driving innovation and economic growth within the European Union.

The EUCC regulation was published on February 7, 2024, and came into force on the twentieth day following that of its publication in the Official Journal of the European Union. The regulation is set to be applied 12 months after it’s the day it came into force, and therefore from February 27, 2025, the EUCC will officially be implemented and operational, as mentioned in articles 49 and 50 of regulation (EU) 2024/482. During this period, relevant stakeholders, including certification bodies and national cybersecurity certification authorities, will need to prepare for compliance with the new requirements established by the EUCC. This includes establishing processes for certification, training personnel, and ensuring that all necessary documentation and standards are in place to support the certification of ICT products and protection profiles.

2.2.3 Stakeholder Involvement

Stakeholder involvement is essential for the successful implementation and ongoing effectiveness of the EUCC, ensuring that diverse perspectives and expertise contribute to the certification process. Each stakeholder group is assigned specific tasks aligned with their expertise and role, ensuring that every aspect of the EUCC certification process is handled by those best suited for the job. By distributing responsibilities in this way, the process becomes more organized and efficient, with each group contributing their knowledge and skills towards a common goal. This structured collaboration not only enhances the effectiveness of the certification process but also accelerates its implementation, ultimately leading to a more robust and successful outcome. The primary stakeholder groups are:

2.2.4 Market Surveillance

Market surveillance plays a pivotal role in maintaining the integrity and effectiveness of the EUCC certification in the digital landscape. It involves the continuous monitoring of certified Information and Communication Technology (ICT) products and services to ensure compliance with relevant regulations and security standards. Market surveillance authorities are tasked with verifying that products meet the established requirements throughout their lifecycle, assessing performance in real-world scenarios, and identifying potential vulnerabilities or non-compliance issues. By conducting assessments and investigations, these authorities can take corrective actions, such as suspending certificates or notifying manufacturers of necessary remedial measures, which further fortifies the cybersecurity framework.

Moreover, effective market surveillance leverages the collaboration between various stakeholders, including certification bodies, national cybersecurity certification authorities, and private sector entities. This multi-dimensional approach enhances the capacity to detect and address emerging threats in a timely manner, as it combines insights from different sectors, enables information sharing, and fosters a proactive stance towards cybersecurity challenges. In this way, market surveillance not only protects consumers and businesses but also supports the credibility of the certification process itself, ensuring that certified products uphold the highest security standards in a rapidly evolving digital landscape.

2.3 Key Features of EUCC

2.3.1 Alignment with International Standards

Evaluations performed under the EUCC scheme shall adhere to the following standards: the Common Criteria and the Common Evaluation Methodology as mentioned in article 3 of regulation (EU) 2024/482. While the Common Criteria and the Common Evaluation Methodology focus broadly on IT products, the EUCC scheme specifically targets ICT products.

In addition, the certification of ICT products under the EUCC scheme is carried out against the security target defined by the applicant or incorporating a certified protection profile, provided the ICT product falls within the category covered by that profile, as specified in Article 5 of Regulation (EU) 2024/482. Protection profiles are certified solely for use in certifying ICT products within the corresponding category. Moreover, as stated in Article 6 of Regulation (EU) 2024/482, the EUCC scheme does not permit conformity self-assessment, as outlined in Article 53 of Regulation (EU) 2019/881 (Cybersecurity Act), ensuring a more rigorous approach to certification and further alignment with international standards and practices.

2.3.2 SOG-IS Mutual Recognition Agreement

The Senior Officials Group - Information Systems Security (SOG-IS) plays a pivotal role in the European cybersecurity landscape through its Mutual Recognition Agreement (MRA), which streamlines the certification and evaluation of Information Technology (IT) security products across participating countries. The SOG-IS MRA ensures that IT products and protection profiles, once evaluated and certified under agreed-upon standards like the

Common Criteria (CC), are recognized across borders without the need for re-evaluation. Fostering trust in the security of these products, eliminates redundant certification processes, and improves the availability of secure IT solutions. Participation in SOG-IS is limited to governmental organizations or agencies within the European Union (EU) and European Free Trade Association (EFTA) countries, maintaining a focus on public trust and security by excluding purely commercial certification bodies.

Building upon this foundation, the European Common Criteria-based cybersecurity certification scheme (EUCC) has been developed, deeply intertwined with the principles and frameworks of the SOG-IS MRA. The EUCC leverages the mutual recognition processes established by SOG-IS, particularly those focusing on ICT security evaluations under the Common Criteria framework. Both the EUCC and SOG-IS MRA utilize the Common Criteria standards, ensuring consistency in the evaluation methodologies and harmonizing certification processes across the EU. This alignment not only simplifies market access for products certified under national SOG-IS schemes but also ensures that products certified under the EUCC are recognized by other SOG-IS participating countries, fostering reciprocal acceptance.

Moreover, the EUCC embodies a policy alignment with the SOG-IS MRA’s objectives, enhancing cybersecurity while integrating national and EU-level efforts into a unified certification approach. By doing so, the EUCC strengthens the regulatory framework for cybersecurity within the EU while maintaining coherence with established international practices under SOG-IS. This interconnected relationship ultimately supports greater trust, security, and efficiency in ICT certification across European and international markets.

2.3.4 Assurance Levels

Certification bodies (CBs) shall issue EUCC certificates at either the ‘substantial’ or ‘high’ assurance level. EUCC certificates at the ‘substantial’ assurance level correspond to certificates covering assurance vulnerability analysis (AVA_VAN) level 1 or 2, while those at the ‘high’ assurance level correspond to certificates covering AVA_VAN level 3, 4, or 5.

The assurance level specified in an EUCC certificate must clearly differentiate between the conformant and augmented use of assurance components, as defined in the Common Criteria. An augmentation involves additional assurance components beyond the standard evaluation assurance level but is not represented by a ‘+’ symbol, as is typical in other contexts. Instead, all augmented components must be explicitly listed and described in detail in the certification report.

Furthermore, the assurance level confirmed in an EUCC certificate may include an evaluation assurance level, providing additional information about the depth of the assessment performed. If no augmentation is included, the certificate will indicate either “the specific assurance package” or “the assurance package conformant to a protection profile,” depending on whether it references a protection profile without specifying an evaluation assurance level, as mentioned in Annex VIII of Regulation (EU) 2024/482.

Additionally, conformity assessment bodies are required to apply the assurance components on which the selected AVA_VAN level depends, as specified in the standards referred to in Article 3 of Regulation (EU) 2024/482.

2.4 Roles of Stakeholders

Within the framework of the European Common Criteria-based cybersecurity certification scheme (EUCC), a diverse array of stakeholders plays a crucial role in ensuring the integrity, reliability, and effectiveness of the certification process. Each stakeholder brings unique expertise and responsibilities that contribute to a comprehensive and robust cybersecurity ecosystem. The involvement of multiple stakeholders is essential, as it fosters collaboration, enhances transparency, and ensures that various perspectives and competencies are integrated into the certification process. This multi-faceted approach not only strengthens the overall security posture of certified products but also builds trust among users, manufacturers, and regulatory bodies, ultimately promoting a safer digital environment across the European Union.

As specified in Article 43 of Regulation (EU) 2024/482, all parties that are part of the EUCC certification process, must ensure the protection of business secrets and other confidential information including trade secrets as well as the preserving it intellectual property rights and take the necessary and appropriate technical and organizational measures.

Particularly the certification bodies and ITSEFs must maintain a secure record system containing all documents related to each evaluation and certification they conduct. These records must be stored securely for at least five years after the withdrawal of the relevant EUCC certificate. If a new EUCC certificate is issued under Article 13(2)(c), the documentation of the withdrawn certificate must be retained alongside the new one for its entire validity period, as stated in Article 40 of Regulation (EU) 2024/482.

2.4.1 Certification Holder

The holder of the EUCC Certificate is responsible for performing the appropriate tasks to monitor the conformity of the certified ICT product with its security requirements, as specified in Article 27 of Regulation (EU) 2024/482. First of all, they shall keep track of vulnerabilities related to the certified ICT product and its known dependencies by looking out for reports or submissions made by users or security researchers, as mentioned in Article 55(1)(c) of Regulation (EU) 2019/881, as well as reviewing vulnerability information shared by other sources. Apart from that the holder of the certificate shall regularly check if the certificate's assurance level remains valid. To do so, the holder must work in cooperation with the certification body (CB), the ITSEF and the national cybersecurity certificate authority to support their monitoring activities.

As specified in Article 41 of Regulation (EU) 2024/482, the holder of the EUCC certificate shall store securely the following for at least five years after the certificate is withdrawn:

1. Records of the information provided to the CB and ITSEF during the certification process.
2. A sample of the certified ICT product.

Upon request by the CB or the national cybersecurity certification authority, the holder must make available the above records and copies to them.

In case of a new EUCC certificate issuance, that replaces an old one, the holder must keep the records of the old certificate along with the new one for as long as the new certificate is valid. In accordance with Article 13(2), point (c), when a new certificate is issued, the scope remains identical and the validity period is extended, therefore during the review process of the certificate, there might be the need to compare the two versions.

The holder of the EUCC certificate must comply with all obligations outlined in Regulation (EU) 2024/482 and Regulation (EU) 2019/881. In the event of non-compliance, the CB is responsible for taking corrective measures as specified in Article 29 of Regulation (EU) 2024/482. If the CB determines that the holder of the EUCC certificate or an applicant for certification has failed to fulfil their commitments and obligations under Articles 9(2), 17(2), 27, and 41 of Regulation (EU) 2024/482, or has not complied with Article 56(8) of Regulation (EU) 2019/881 or Chapter VI of Regulation (EU) 2024/482, the CB shall grant a period of no more than 30 days for the holder to implement remedial actions.

Should the holder fail to take appropriate corrective measures within the specified timeframe, the certification body may suspend the EUCC certificate in accordance with Article 30 or withdraw it under the provisions of Articles 14 and 20. In cases where non-compliance is persistent or repeated, the EUCC certificate shall be withdrawn in accordance with Articles 14 and 20 of Regulation (EU) 2024/482.

Furthermore, the CB is required to notify the national cybersecurity certification authority of any findings related to non-compliance. If the identified non-compliance also affects the fulfillment of requirements under other relevant Union legislation, the national cybersecurity certification authority must immediately inform the appropriate market surveillance authority to ensure coordinated enforcement and regulatory action.

2.4.2 National Cybersecurity Certification Authority

The national cybersecurity certification authority must notify the European Commission about the certification bodies (CB) within its territory that are authorized to certify products at the assurance level "substantial" and "high". For those that are authorized to certify products with "substantial" assurance level, the notification is based on the accreditation of these CB. But for the ones authorized to certify products with "high" assurance level, the notification depends also on the specific authorization decision made for the CB. Apart from the assurance level or levels the CB is competent to issue EUCC certificates, the national cybersecurity certification authority shall also provide information related to accreditation such as:

1) The accreditation date, reference number, scope and duration of validity.
2) The name, address and country of registration of the CB.
3) Information about the national accreditation body.
4) For authorization of level “high” they should also include the date, reference number, and duration of validity of the authorization. As well as, he scope of the authorization including the highest AVA_VAN level and if applicable the covered technical domain.

After the national cybersecurity certification authority informed the European Commission about the CBs, must send a copy of the notification to ENISA, so they publish accurate information on the cybersecurity certification website, that would be used as a means of proving the eligibility of the CBs.

The national cybersecurity certification authority shall promptly review any changes in accreditation status and, in the event of withdrawal, notify the Commission and may request further action under Article 61(4) of Regulation (EU) 2019/881. All notifications and actions described above shall be conducted in accordance with Article 23 of Regulation (EU) 2024/482.

In addition to the requirements outlined in Article 23, the national cybersecurity certification authority shall also notify the European Commission and ENISA about Information Technology Security Evaluation Facilities (ITSEFs). This notification shall include the address of the ITSEF, its valid accreditation, and, where applicable, the valid authorization of the ITSEF, as per the obligations set out in Article 24 of Regulation (EU) 2024/482.

In accordance with Article 25 of Regulation (EU) 2024/482, the national cybersecurity certification authority shall monitor compliance with this Regulation and Regulation (EU) 2019/881. This includes oversight of:

1) CBs and ITSEFs, ensuring they fulfill their obligations.
2) Holders of EUCC certificates, verifying their continued compliance.
3) Certified ICT products, confirming adherence to EUCC requirements.
4) The assurance provided by EUCC certificates in relation to evolving cybersecurity threats.

To conduct its monitoring activities, the national cybersecurity certification authority shall rely on:

1) Information from certification bodies, national accreditation bodies, and market surveillance authorities.
2) Audits, investigations, and sampling based on risk assessments.
3) Complaints received from relevant stakeholders.

Each year, in collaboration with other market surveillance authorities, the national cybersecurity certification authority shall sample at least 4% of EUCC certificates, selected using objective criteria such as product category, assurance level, CB, and relevant information received. The authority shall inform certificate holders of the selected ICT products and the selection criteria.

If an ICT product is suspected of non-compliance, the CB responsible, assisted by the respective ITSEF, shall conduct an additional review as per Annex IV, Section IV.2 and report the findings. Where necessary, the national cybersecurity certification authority may launch investigations or use its monitoring powers under Article 58(8) of Regulation (EU) 2019/881.

In case of cross-border investigations involving ICT products certified by bodies in other Member States, the national cybersecurity certification authority shall inform the relevant national authorities and notify the European Cybersecurity Certification Group.

2.4.3 Certification Bodies

A certification body (CB) must be authorized by the national cybersecurity certification authority to issue EUCC certificates at the assurance level "high”, in accordance with article 21 of Regulation (EU) 2024/482. This authorization is granted only if the CB, in addition to meeting the accreditation requirements set out in Article 60(1) and the Annex to Regulation (EU) 2019/881, also complies with the following conditions:

1) It possesses the required expertise and competence to make certification decisions at the assurance level "high”.
2) It carries out its certification activities in collaboration with an ITSEF that has been authorized in accordance with Article 22.
3) It implements the necessary technical and operational measures to effectively protect confidential and sensitive information for assurance level "high," in addition to the requirements outlined in Article 43.

The national cybersecurity certification authority is responsible for assessing whether a CB meets these requirements. This assessment includes structured interviews and a review of at least one pilot certification performed under this Regulation. When conducting the assessment, the national cybersecurity certification authority may reuse relevant evidence from prior authorizations or similar activities granted under:

1) This Regulation.
2) Any other european cybersecurity certification scheme adopted under Article 49 of Regulation (EU) 2019/881.
3) A national scheme referred to in Article 49 of this Regulation.

After the national cyber security certification authority has completed the evaluation, they must produce an authorization report which is subject to peer assessment review in accordance with article 59 of regulation (EU) 2019/881. This report should specify the ICT product categories and protection profiles to which the authorization extends. The authorization should not be valid for period longer than the validity of the accreditation. The authorization can be renewed upon request if the CB continues to meet the requirements stated above, on this instance no pilot evaluation is required.

If the national cyber security certification authority finds the CB to not be compliant with the conditions set out above, they are responsible to withdraw the authorization. Upon withdrawal, the CB must under no circumstances promote itself as being an authorized CB.

In accordance with article 26 of Regulation 2024/482, a CB is responsible for monitoring compliance and ensuring that the ICT products certified continue to meet security requirements. Specifically, the certification body shall oversee:

1) The compliance of certificate holders with their obligations under Regulation (EU) 2019/881 and Regulation (EU) 2024/482 concerning the EUCC certificate issued by the CB.
2) The compliance of certified ICT products with the applicable security requirements.
3) The assurance expressed in the certified protection profiles.

The CB shall conduct its monitoring activities based on:

1) Information provided by applicants as part of their commitments under Article 9(2).

2) Findings from other relevant market surveillance authorities.
3) Complaints received.
4) Vulnerability information that may impact certified ICT products.

Additionally, the national cybersecurity certification authority may establish rules for periodic dialogue between CBs and EUCC certificate holders. This dialogue aims to verify and report on compliance with commitments made under Article 9, without prejudice to activities carried out by other relevant market surveillance authorities.

The CB is also responsible for identifying non-conformity and request appropriate remediation actions from the certificate holders, as was mentioned in Article 28 of Regulation 2024/482. When a certified ICT product or protection profile fails to meet the requirements set out in this Regulation and Regulation (EU) 2019/881, the CB shall:

1) Inform the certificate holder about the identified non-conformity and request corrective measures.
2) If the non-conformity impacts compliance with other relevant Union legislation that recognizes the EUCC certificate as a presumption of conformity, the CB shall promptly notify the national cybersecurity certification authority, which will then inform the relevant market surveillance authority.
3) Require the certificate holder to propose a remedial action plan within a maximum of 30 days.
4) If necessary, suspend the EUCC certificate without undue delay in accordance with Article 30, particularly in emergency cases or when the certificate holder fails to cooperate.
5) Assess the proposed remedial actions in accordance with Articles 13 and 19 to determine their adequacy.
6) If the certificate holder fails to propose sufficient remedial actions within the given timeframe, the EUCC certificate shall be suspended (under Article 30) or withdrawn (under Articles 14 or 20).

2.4.4 ITSEF

An Information Technology Security Evaluation Facility (ITSEF) plays a critical role in the evaluation of ICT products subject to certification under the EUCC. ITSEFs must meet specific accreditation and authorization requirements to ensure they possess the necessary expertise and technical capabilities to conduct evaluations, particularly for ICT products certified at the "high" assurance level. As set out in Article 22 of Regulation (EU) 2024/482, an ITSEF must be authorized by the national cybersecurity certification authority before it can carry out evaluations for products at this assurance level.

To obtain authorization, an ITSEF must first demonstrate compliance with the accreditation requirements outlined in Article 60(1) and the Annex to Regulation (EU) 2019/881. Additionally, the ITSEF must meet the following conditions:

1) Must have the needed expertise to assess an ICT’s product resistance to state-of-the-art cyber-attacks guarding the out by actors with significant skills and resources, by performing the necessary evaluation activities.
2) Demonstrate competence in performing evaluation activities that systematically assess a target of evaluation’s resilience against skilled attackers, assuming an attack potential of "moderate" or "high", as defined in Article 3.

3) Implement appropriate technical and operational measures to ensure the effective protection of confidential and sensitive information when evaluating products at the **"high"** assurance level, in addition to meeting the security requirements set out in Article 43.

The national cyber security certification authority is responsible to assess the fulfillment of the above requirements by the ITSEF. The assessment would consist of structured interviews, and they would also review at least one pilot evaluation performed by the ITSEF in accordance with the Regulation (EU) 2024/482. Furthermore, the authority may consider prior authorizations or similar assessments performed under:

1) This Regulation.
2) Another European cybersecurity certification scheme established under Article 49 of Regulation (EU) 2019/881.
3) A national certification scheme referenced in Article 49 of Regulation (EU) 2024/482.

After the national cyber security certification authority has completed the evaluation, they must produce an authorization report which is subject to peer assessment review in accordance with article 59 of regulation (EU) 2019/881. This report should specify the ICT product categories and protection profiles to which the authorization extends. The authorization should not be valid for period longer than the validity of the accreditation. The authorization can be renewed upon request if the ITSEF continues to meet the requirements stated above, on this instance no pilot evaluation is required.

If the national cyber security certification authority finds the ITSEF to not be compliant with the conditions set out above, they are responsible to withdraw the authorization. Upon withdrawal, the ITSEF must under no circumstances promote itself as being an authorized ITSEF.

2.4.5 ENISA

The European Union Agency for Cybersecurity (ENISA) plays a key role in maintaining and publishing information related to EUCC certificates. As specified in Article 42 of Regulation (EU) 2024/482, ENISA shall publish the following information on the cybersecurity certification website referred to in Article 50(1) of Regulation (EU) 2019/881:

1) All issued EUCC certificates.
2) The current status of the EUCC certificates, stating whether it is in force, suspended, withdrawn, or expired.
3) For every EUCC certificate, the corresponding certification reports.
4) A list of accredited conformity assessment bodies.
5) A list of authorized conformity assessment bodies.
6) The state-of-the-art (SOTA) documents.
7) The opinions of the European cybersecurity certification group as they were mentioned in article 62 of regulation (EU) 2019/881.
8) All peer assessment reports issued in accordance with article 47.

The above information shall be made available at least in English.

Certification bodies and where applicable national cybersecurity certification authorities are responsible to inform ENISA without any delay, about their decisions that may affect the status or content of an EUCC certificate, so they can update the respective information listed on the cybersecurity certification website. Additionally, ENISA must ensure that the published information clearly specifies the product versions covered by each EUCC certificate.

2.5 Certification of ICT products

2.5.1 Evaluation Criteria and Methods

The certification of ICT products follows strict evaluation criteria and methodologies to ensure compliance with security standards. As outlined in Article 7 of Regulation (EU) 2024/482, an ICT product submitted for certification must, at a minimum, be evaluated based on:

1) The application elements of the EUCC standard, as they described in Article 3.
2) The security assurance requirements classes for vulnerability assessment and independent functional testing, as mentioned in the evaluation standards of Article 3.
3) The risk level associated with the intended use of the ICT product, as determined under Article 52 of Regulation (EU) 2019/881, and its security functions supporting the security objectives set out in Article 51 of the same regulation.
4) The relevant state-of-the-art documents listed in Annex I of Regulation 2024/482.
5) The certified protection profiles applicable to the product, as listed in Annex II of Regulation 2024/482.

Exceptional Cases and Exemptions

In exceptional and duly justified cases, a conformity assessment body (CAB) may request to refrain from applying a relevant state-of-the-art document. According to Article 7 of Regulation (EU) 2024/482 in such cases:

1) The CAB shall inform the national cybersecurity certification authority with a duly reasoned for their request.
2) The national cybersecurity certification authority then must assess the justification for an exception, and where justified, approve it.
3) While the CAB waits for the decision of the national cybersecurity certification authority shall not issue any certificates.
4) If approved, the national cybersecurity certification authority must notify the European Cybersecurity Certification Group (ECCG), which may issue an opinion.
5) The national cybersecurity certification authority shall take utmost account of the ECCG's opinion when making its final decision.

Certification at AVA_VAN Levels 4 and 5

Certification of ICT products at AVA_VAN level 4 or 5 is only possible under specific conditions, as specified in Article 7 of Regulation (EU) 2024/482:

If the ICT product falls within a technical domain listed in Annex I of Regulation 2024/482, it must be evaluated in accordance with the applicable state-of-the-art (SOTA) documents for that domain.

<u>SOTA on Technical Domain "Smart Cards & Similar Devices"</u>

1) Minimum ITSEF requirements for security evaluations of smart cards and similar devices (Approved by ECCG on 20 October 2023, Version 1.1)

This document outlines the essential capabilities that accredited IT Security Evaluation Facilities (ITSEFs) must possess to evaluate smart cards and similar devices. It specifies the required knowledge, skills, equipment, and methodologies necessary to conduct security evaluations, particularly focusing on attack scenarios described in related state-of-the-art documents. While it doesn't guide the evaluation process itself, it ensures ITSEFs meet the minimum standards to effectively assess integrated circuits, crypto libraries, platforms, and integrated circuit cards.

2) Minimum Site Security Requirements (Approved by ECCG on 20 October 2023, Version 1.1)

This document defines the baseline security controls developers must implement and evaluators must verify to ensure the confidentiality and integrity of ICT products, particularly smart cards and similar devices, under the EUCC scheme. It aligns with the Common Evaluation Methodology (CEM) and focuses on meeting ALC_DVS.1 and ALC_DVS.2 (Life-cycle Support, Developer environment security) requirements, essential for evaluations involving high attack potential (AVA_VAN.5). The document outlines mandatory security objectives, policies, and measures for development environments, ensuring consistency across site audits and compliance with established standards like ISO/IEC 27001, while allowing for justified adaptations based on risk assessments.

3) Application of Common Criteria to integrated circuits (Approved by ECCG on 20 October 2023, Version 1.1)

This document provides guidance on applying Common Criteria (CC) assurance to integrated circuits (ICs), particularly focusing on security evaluations at the AVA_VAN.5 level. It addresses the growing complexity and risks associated with microchips in modern information technology, emphasizing the importance of effective security measures at both the system and chip levels. Aimed at manufacturers, evaluators, and certifiers, it ensures that CC is applied consistently with state-of-the-art hardware evaluations, promoting transparency in security assurance for hardware components.

4) Security Architecture requirements (ADV_ARC) for smart cards and similar devices (Approved by ECCG on 20 October 2023, Version 1.1)

This document outlines the requirements for developers and evaluators regarding the application of the ADV_ARC family of security assurance requirements for smart cards, similar devices, and Secure Sub-Systems (3S) within System-on-Chip (SoC) environments. It provides guidance on the security architecture required for these devices, with a focus on high-security devices operating at an AVA_VAN.5 level. The document specifies the mandatory information that the ARC document (developer documentation) should include, detailing how security architecture properties such as self-protection, domain separation, and non-bypass ability are to be designed, described, and assessed.

Considering Smart Cards and Similar Devices, the document covers the security architecture of Integrated Circuits (ICs) with embedded software implementing cryptographic services, including transition from low-function mode to secure mode during operation, with a focus on protecting against attackers with high attack potential. Also, regarding Secure Sub-Systems (3S) in SoC, the document extends the principles of security architecture to secure sub-systems within a System-on-Chip (SoC), including IP blocks, cryptography services, and memory management. It outlines how these systems should *protect high-value assets and support secure boot processes, with an emphasis on recovery modes if the system fails to load properly.*

5) Certification of “open” smart card products (Approved by ECCG on 20 October 2023, Version 1.1)

This document defines key concepts related to the evaluation of smart cards and similar devices under the EUCC scheme, specifically focusing on the composition of evaluation results. It introduces the distinction between platforms, ranging from open, closed, to isolating platforms, and explains terms like “known” and “unknown” applications, which refer to applications evaluated as part of the original architecture and those added post-evaluation, respectively. The document provides clarity on how these concepts influence the evaluation of integrated circuits, software operating systems, and applications within the context of certification.

6) Composite product evaluation for smart cards and similar devices (Approved by ECCG on 20 October 2023, Version 1.1)

This document clarifies the evaluation process when hardware and software components are developed separately but integrated into a final product. Unlike the ACO assurance class, which is limited to lower assurance levels, this methodology supports high-level assurance evaluations, suitable for sensitive applications such as banking or digital signatures. The evaluation ensures that the interaction between the platform (hardware and OS) and application does not introduce vulnerabilities, reusing platform evaluation results where applicable. The document also applies to any secure ICT product involving independently evaluated components integrated into a final composite product.

7) Application of Attack Potential to Smartcards (Approved by ECCG in August 2023, Version 1.2)

This document, supporting the EUCC scheme, interprets the Common Criteria Methodology (CEM) based on smartcard evaluation expertise and industry input from the International Security Certification Initiative (ISCI) and JIL Hardware Attacks Subgroup (JHAS) of SOG-IS. It provides guidance metrics for calculating the attack potential necessary for an attacker to successfully compromise a smartcard or similar device. The focus is on evaluating the total effort required for an attack based on the operational behavior of the device, rather than hardware or software-specific applications.

<u>SOTA on Technical Domain "Hardware Devices with Security Boxes"</u>

1) Minimum ITSEF requirements for security evaluations of hardware devices with security boxes (Approved by ECCG on 20 October 2023, Version 1.1)

This document outlines the essential skills and knowledge required for evaluators performing physical evaluations of hardware devices with security boxes (HDwSB). It covers the understanding of secure physical technology, attack techniques, and the tools needed for vulnerability and failure analysis. Evaluators must be familiar with hardware principles, microcontroller architecture, and various attack techniques such as side channel attacks, fault injection, and cryptographic attacks. The document also details the necessary equipment—ranging from standard to specialized tools—needed to conduct thorough evaluations and exploit potential weaknesses in HDwSB designs.

2) Minimum Site Security Requirements (Approved by ECCG on 20 October 2023, Version 1.1)

The same SOTA document as the as technical domain "Smart Cards & Similar Devices".

3) Application of Attack Potential to hardware devices with security boxes (Approved by ECCG in August 2023, Version 1.2)

This document, supporting the EUCC scheme, interprets the Common Criteria Methodology (CEM) with a focus on the "Hardware Devices with Security Boxes" technical domain, drawing on evaluation experience and industry input from the JIL Embedded Devices Subgroup (JEDS) of SOG-IS. It provides guidance on calculating the attack potential required for an attacker to successfully compromise such devices, focusing on their operational behavior as defined in the related Security Target. The document includes attack potential ratings and parameters for most attacks, with additional details on software attacks and attacks on Random Number Generators (RNG) to be covered in future revisions

If the ICT product belongs to a category covered by a certified protection profile (including AVA_VAN level 4 or 5) that has been listed as a state-of-the-art protection profile in Annex II of Regulation 2024/482, it must be evaluated using the specified evaluation methodology. If neither of the above applies, certification is only possible in exceptional and duly justified cases, subject to approval by the national cybersecurity certification authority.

In such exceptional cases, the CBA must notify the national cybersecurity certification authority with a justification and a proposed evaluation methodology. The authority will then:

1) Assess the justification and either approve or amend the methodology.
2) Prohibit the CAB from issuing any certificate until a decision is made.
3) Report the intended certification to the European Cybersecurity Certification Group, which may issue an opinion.

The national cybersecurity certification authority shall take utmost account of the ECCG's opinion before making its final decision.

Composite Product Evaluations

For ICT products undergoing a composite product evaluation, the ITSEF responsible for evaluating the underlying ICT product must share relevant information with the ITSEF performing the evaluation of the composite ICT product, as required by state-of-the-art documents, according to Article 7 of Regulation (EU) 2024/482.

2.5.2 Prerequisites for Certification

To obtain certification under the EUCC, applicants must ensure the provision of comprehensive, accurate, and verifiable information to both the certification body and the ITSEF (Information Technology Security Evaluation Facility). According to Article 8 of Regulation (EU) 2024/482 the applicant for certification must:

1) Provide or make available to the CB and the ITSEF all necessary information requested during the certification activities, including:
    a. A link to their website containing supplementary cybersecurity information, as per Article 55 of Regulation (EU) 2019/881.
    b. A detailed description of their vulnerability management and vulnerability disclosure procedures.
2) The submitted information must include all relevant evidence aligned with the 'Developer action elements' as specified in the Common Criteria (CC) and Common Evaluation Methodology (CEM) and follow the formats outlined in the 'Content and

Presentation of Evidence' sections corresponding to the selected assurance level and related security assurance requirements. This includes, where applicable, detailed information about the ICT product and its source code, subject to safeguards against unauthorized disclosure.

3) Applicants can submit relevant evaluation results from prior certifications, provided they are applicable to the current certification process. This includes certifications under:
    a. This regulation.
    b. Other European cybersecurity certification scheme adopted under Article 49 of Regulation (EU) 2019/881.
    c. A national scheme referred to in Article 49 of Regulation (EU) 2024/482.

    The ITSEF may reuse evaluation results provided they are relevant to the current certification, conform to applicable requirements, and their authenticity has been verified.

4) If the CB authorizes a product to undergo composite product certification, applicants must submit all necessary elements in accordance with the applicable state-of-the-art documents.

2.5.3 Conditions for Issuance

For the Certificate Body (CB) to issue a EUCC certificate, the following conditions must be met, as mentioned in Article 9 of of Regulation (EU) 2024/482:

1) The category of the ICT product falls within the scope of both the accreditation and, where applicable, the authorization of the certification body and the Information Technology Security Evaluation Facility (ITSEF) involved in the certification process.
2) The applicant for certification has duly signed a formal statement undertaking all obligations.
3) The ITSEF has completed the evaluation without raising any objections.
4) The certification body has conducted a comprehensive review of the evaluation results and has identified no objections.
5) The certification body has verified that the evaluation technical reports submitted by the ITSEF are consistent with the supporting evidence provided and that the evaluation standards, criteria, and methodologies have been accurately and appropriately applied.

As mentioned above, the applicant for certification, is responsible to sign a formal statement after concluding the following obligations:

1) To provide the CB and the ITSEF with all necessary, complete, and accurate information, and to furnish any additional information as required upon request.
2) To refrain from promoting the ICT product as certified under the EUCC prior to the official issuance of the EUCC certificate.
3) To represent the ICT product as certified solely within the scope defined in the EUCC certificate.
4) To immediately discontinue any promotion of the ICT product as certified in the event of suspension, withdrawal, or expiration of the EUCC certificate.
5) To ensure that all ICT products marketed or sold with reference to the EUCC certificate are strictly identical to the ICT product that was subject to the certification process.
6) To comply with the rules governing the use of the EUCC certificate's mark and label.

2.5.4 Contents of EUCC Certificate

As mentioned in Annex VII of Regulation (EU) 2024/482, the EUCC Certificate must contain:

1) A unique identifier assigned by the CB responsible for issuing the certificate.
2) Information related to the certified ICT product or protection profile and the certificate holder, including:
    a. The name of the ICT product or PP and, where applicable, the TOE.
    b. The type of ICT product or PP and, where applicable, the TOE.
    c. The version of the ICT product or PP.
    d. The name, address, and contact details of the certificate holder.
    e. A hyperlink to the certificate holder's website containing the supplementary cybersecurity information.
3) Information related to the evaluation and certification of the ICT product or protection profile, including:
    a. The name, address, and contact details of the CB that issued the certificate.
    b. Where different from the CB, the name of the ITSEF responsible for conducting the evaluation.
    c. The name of the competent national cybersecurity certification authority.
    d. A reference to this Regulation.
    e. A reference to the certification report associated with the certificate.
    f. The applicable assurance level.
    g. A reference to the version of the standards applied during the evaluation.
    h. Identification of the assurance level or package, including the assurance components applied, and the AVA_VAN level covered.
    i. Where applicable, references to one or more PPs with which the ICT product or PP complies.
    j. The date of issuance of the certificate.
    k. The period of validity of the certificate.
4) The mark and label associated with the certificate. They must be affixed visibly, legibly, and indelibly to the certified ICT product or its data plate. For software products, the mark and label must appear in the accompanying documentation or be easily accessible via a website, as was stated in Article 11 of Regulation 2024/482. The mark and label shall include:
    a. The assurance level and AVA_VAN level of the certified ICT product.
    b. A unique certificate identification, including the scheme name, the certification body's accreditation reference, the year and month of issuance, and an identification number assigned by the certification body.
    c. A QR code linking to a website with information on the certificate's validity, certification details, publicly available cybersecurity information, and, where applicable, historical certification data for traceability.

In addition to the above, according to Article 10 of EUCC Regulation, the scope and boundaries of the certified ICT product shall be unambiguously specified in the EUCC certificate or the certification report. This specification shall clearly indicate whether the entire ICT product has been certified or only specific parts thereof.

The CB shall provide the applicant with the EUCC certificate at least in electronic form to ensure timely and efficient delivery. Furthermore, the CB is required to produce a certification report for each EUCC certificate it issues. This certification report shall be based on the evaluation technical report prepared by the ITSEF. Both the evaluation technical report and the certification report must clearly indicate the specific evaluation criteria and methods that were applied during the evaluation process.

Lastly, the CB shall provide the national cybersecurity certification authority and ENISA with electronic copies of every EUCC certificate and the corresponding certification report to ensure regulatory compliance and facilitate centralized record-keeping.

2.5.5 Period of Validity of an EUCC Certificate

The Certificate Body (CB) is responsible for setting the validity period for every EUCC certificate issued by them, considering the characteristics of the certified ICT product. The period of validity must not exceed the period mark of 5 years, as it has been stated in Article 12 of Regulation (EU) 2024/482. An exception to this where the validity period could exceed 5 years, is subject to the approval of the national cybersecurity certification authority. When the exception applies, the national cybersecurity certification authority must notify the European cybersecurity certification group of the granted approval without no delay.

2.5.6 Review of EUCC Certificate

Article 13 or Regulation (EU) 2024/482 details the process for reviewing an EUCC certificate. The certification body (CB) may initiate a review of the certificate for an ICT product either upon the request of the certificate holder or for other justified reasons. This review must be conducted in accordance with Annex IV of the same regulation, and the CB will determine its scope. Annex IV includes reassessing whether an unchanged certified product meets its security requirements, evaluating the impact of changes on certification, reviewing patch applications if covered by the certification, and examining lifecycle or production processes. If necessary, the CB may request the ITSEF to carry out a re-evaluation of the certified ICT product. Based on the outcomes of the review and, if applicable, the re-evaluation, the certification body may take one of several actions:

1) Confirm the EUCC certificate.

2) Withdraw it in accordance with Article 14 of Regulation (EU) 2024/482.

3) Withdraw it and issue a new certificate with the same scope but an extended validity period.

4) Withdraw it and issue a new certificate with a different scope.

Additionally, the CB has the authority to suspend the EUCC certificate without undue delay, in accordance with Article 30, pending remedial actions by the certificate holder.

2.5.7 Handling Non-Compliance

In the broader regulatory framework, a Conformity Assessment Body (CAB) refers to any entity responsible for evaluating whether products, services, or systems meet specified standards. However, in the context of EU cybersecurity certification, the term does not represent a distinct entity. Instead, the CAB consists of Certification Bodies (CBs) and Information Technology Security Evaluation Facilities (ITSEFs), which are the recognized entities performing conformity assessment activities under Regulation (EU) 2024/482, and any instance of non-compliance is subject to corrective action as outlined in Article 31.

If a CB fails to comply with its obligations, or if a CB identifies non-compliance by an ITSEF, the national cybersecurity certification authority must take immediate action to assess and mitigate the potential impact. According to Article 31(1), the authority shall:

1) Identify potentially affected EUCC certificates, with the support of the concerned ITSEF.
2) Where necessary, request additional evaluation activities on one or more ICT products or protection profiles. These evaluations may be carried out by the original ITSEF that perform the evaluation or if applicable, any other accredited and authorized ITSEF with the necessary technical expertise.
3) Analyze the impact of non-compliance.
4) Notify the holder of the EUCC certificate affected by non-compliance.

Following this assessment, the CB must determine the appropriate course of action regarding the impacted certificates. As stated in Article 31(2), the CB may either:

1) Maintain the EUCC certificate without changes if no significant risk is identified.
2) Withdraw the EUCC certificate in accordance with Article 14 or Article 20 and, where appropriate, issue a new EUCC certificate.

In addition, the national cybersecurity certification authority must report cases of CB's or ITSEF's non-compliance, to the national accreditation body when necessary. Where applicable, they should also assess the potential impact on the authorization.

2.5.8 Suspension of Certificate

The suspension of an EUCC certificate is carried out by the certification body (CB) for a period appropriate to the circumstances, as specified in Article 30 of Regulation 2024/482, not exceeding 42 days, starting the day after the suspension decision. This suspension does not affect the validity of the certificate. The CB must promptly notify both the certificate holder and the national cybersecurity certification authority, providing the reasons for the suspension, the required corrective actions, and the duration of the suspension. The certificate holder is responsible for informing purchasers of the affected ICT products about the suspension and its reasons, except for information that could pose a security risk or contains sensitive details. This information must also be made publicly available by the certificate holder. If the certificate is linked to conformity under other relevant Union legislation, the national cybersecurity certification authority must inform the appropriate market surveillance authority. The suspension must also be reported to ENISA in accordance with Article 42(3) of regulation (EU) 2024/482. In exceptional cases, the national cybersecurity certification authority may authorize an extension of the suspension period, but the total duration cannot exceed one year.

2.5.9 Withdrawal of Certificate

According to Article 14 of Regulation (EU) 2024/482, the certification body that issued the certificate is responsible for its withdrawal, without prejudice to Article 58(8)(e) of Regulation (EU) 2019/881. Once the certificate is withdrawn, the certification body must notify the national cybersecurity certification authority, which in turn informs other relevant market surveillance authorities. Additionally, the certification body must notify ENISA to support its responsibilities under Article 50 of Regulation (EU) 2019/881. Furthermore, the holder of an EUCC certificate has the right to request its withdrawal.

2.6 Certification of Protection Profiles

The certification process for Protection Profiles under Regulation (EU) 2024/482 largely mirrors that of ICT products, with some key differences highlighted below.

2.6.1 Information Submission

Applicants for the certification of Protection Profiles must provide all necessary information to the certification body and ITSEF, as stipulated in Article 16 of Regulation (EU) 2024/482. The requirements outlined in Article 8 of the same regulation that refer to ICT products, apply with the necessary adjustments for Protection Profiles.

2.6.2 Evaluation and Issuance

As noted in Article 15 of Regulation (EU) 2024/482, a protection profile may be certified without applying the relevant state-of-the-art documents in exceptional and duly justified cases. In this case, the conformity assessment body (CAB) must inform the national cybersecurity certification authority and provide the justification, evaluation methodology, and await approval before proceeding with the certification. This differs from ICT product certification, where there are also specific procedures but may involve more technical details due to the product's nature.

Similar to ICT product certification, Articles 9 and 10 of Regulation (EU) 2024/482 apply mutatis mutandis as has been stated in Article 17. However, a distinct requirement for Protection Profiles is that the ITSEF evaluates whether the profile is complete, consistent, technically sound, and effective for the intended use and security objectives of the ICT product category it covers. Certification can only be issued by:

1) A national cybersecurity certification authority or another public body accredited as a certification body (CB).
2) A CB with prior approval from the national cybersecurity certification authority for each individual Protection Profile.

2.6.3 Validity Period

The certification body sets the validity period for each EUCC certificate, which may extend up to the lifetime of the Protection Profile itself as has been mentioned in Article 18 of Regulation (EU) 2024/482.

2.6.4 Review of Certificates

Like ICT product certificates, Protection Profile certificates can be reviewed upon request by the certificate holder or for other justified reasons. The conditions for review follow those of ICT product’s and are applied mutatis mutandis in Article 19 of Regulation (EU) 2024/482. Based on the review, the certification body may:

1) Confirm the certificate.
2) Withdraw the certificate.

3) Withdraw and reissue a certificate with identical scope but extended validity.
4) Withdraw and reissue a certificate with a modified scope.

2.6.5 Withdrawal of Certificates

Certificates for Protection Profiles are withdrawn by the certification body that issued them, following procedures mentioned in Article 14 of Regulation (EU) 2024/482, applied mutatis mutandis, as mentioned in Article 20. If the certificate was issued upon prior approval by a national cybersecurity certification authority, it must be withdrawn by the national cybersecurity certification authority that approved it.

2.7 Challenges and Considerations

2.7.1 Industry Adoption

As part of the industry's adoption of the EU Cybersecurity Certification Scheme (EUCC), national cybersecurity certification schemes and their related procedures for ICT products and processes covered by the EUCC will cease to produce effects 12 months after the entry into force of Regulation (EU) 2024/482, as outlined in Article 49(1). However, certification processes may still be initiated under a national scheme within 12 months of the regulation's entry, as long as they are finalized within 24 months, as specified in Article 49(2). Additionally, certificates issued under these national schemes may be subject to review, with new certificates replacing the reviewed ones in accordance with the EUCC, as per Article 49(3).

2.7.2 Global Context

In the context of global cybersecurity certification, third countries that wish to certify their products in accordance with the EU regulations and have their certifications recognized within the Union must enter into a mutual recognition agreement with the European Union. As stated in Article 44(1) of Regulation (EU) 2024/482, such agreements are essential for the certification of ICT products from third countries. These agreements ensure that products certified under these frameworks are recognized as compliant with the European cybersecurity standards, promoting international cooperation and mutual trust.

The mutual recognition agreement must specifically cover the applicable assurance levels for certified ICT products, as well as, where relevant, the protection profiles. Article 44(2) clarifies that the agreement must also outline these technical aspects to ensure that certifications from third countries are aligned with EU standards and requirements.

Moreover, in order for a third country to qualify for a mutual recognition agreement, it must fulfil a set of conditions outlined in Article 44(3). These conditions include having an independent authority that is capable of supervising and monitoring compliance, ensuring that certifications meet the required standards. The authority must be a public body, separate from the entities it oversees, and it should have the necessary powers to conduct investigations, enforce compliance, and impose penalties where appropriate. Additionally, the authority must agree to collaborate with the European Cybersecurity Certification Group (ECCG) and ENISA to share best practices and developments in the field of cybersecurity certification, which is vital to maintaining uniformity and consistency across global certification processes. Also, third countries seeking a mutual recognition agreement must demonstrate that they have an independent accreditation body, as stated in Article 44(3)(b), which performs accreditations using standards equivalent to those set out in Regulation (EC) No 765/2008. This ensures that the accreditation processes of third countries are aligned with EU standards, maintaining the integrity of the certification system.

For third countries seeking recognition at the "high" assurance level, additional requirements must be met. According to Article 44(4), such agreements can only be concluded if the third country has an independent and public cybersecurity certification authority capable of performing or delegating evaluation activities equivalent to those required for national authorities under Regulation (EU) 2024/482 and Regulation (EU) 2019/881. Additionally, a joint mechanism, similar to the EU’s peer assessment process, must be established to facilitate the exchange of practices and collaboratively address issues related to evaluation and certification.

By setting these conditions, the EU aims to ensure that third-country certifications are conducted with the same rigor and standards as those within the Union, fostering international collaboration and the global recognition of the EU cybersecurity certification framework.

2.7.3 EUCC Adaptation to Emerging Technologies

In the context of adapting the EU Cybersecurity Certification Scheme (EUCC) to emerging technologies, as outlined in Article 48(1) of Regulation (EU) 2024/482, the Commission may request the European Cybersecurity Certification Group (ECCG) to adopt an opinion regarding the maintenance of the EUCC and to undertake the necessary preparatory work. Furthermore, the ECCG may endorse state-of-the-art (SOTA) documents, which, once endorsed, shall be published by ENISA.

3. COMMON CRITERIA A PRECURSOR TO EUCC

Common Criteria (CC) are defined as the Common Criteria for Information Technology (IT) Security Evaluation as set out in the international ISO/IEC standard ISO/IEC 15408. In other words, the Common Criteria framework refers to the ISO/IEC 15408, which is used for evaluating the security properties of IT products and services. Throughout this document, these IT products and services will be referred to as Targets of Evaluation (TOE). The Common Criteria framework provides a structured methodology for specifying security requirements, evaluating TOE against those requirements, and certifying that the TOE meets the specified security standards.

The EUCC scheme has been derived from Common Criteria but focuses specifically on ICT TOE that are intended for the European market, hence reassuring these TOE meet the security requirements set by the EU regulations and directives. On the other hand, Common Criteria is an internationally recognized framework for evaluating the security posture of a great variety of TOE. As it is not limited within the EU, this standard can be applied globally in multiple sectors and types of technologies.

The Common Criteria framework operates through a structured and modular approach that allows for flexibility and customization. Its core components consist of:

3.1 Protection Profiles

Protection Profiles (PPs) are recognized internationally under the Common Criteria framework. A PP is a document that depicts a set of security requirements for a specific Targets of Evaluation (TOE) type, like a firewall, smart card, or secure operating system, providing a baseline for evaluation to ensure consistency and comparability across similar TOE during the evaluation process. The primary goal of PPs is to provide a standardized set of security requirements that can be used during the evaluation and certification of TOE that fall under the same category. If the TOE meets those specific security requirements, it will then be certified based on that PP.

3.1.1 Components of Protection Profiles

1) **Security Problem Definition**: Security Problem Definition describes the security environment of the Protection Profile (PP), and includes:
    a. **Threats**: Threats are a collection of potential security threats that the Targets of Evaluation (TOE) category is expected to address.
    b. **Assumptions**: Assumptions are the conditions that are assumed to be true for the specific evaluation, like the operational environment.
    c. **Organizational Security Policies (OSPs)**: OSPs are high-level rules or requirements that must be enforced.
2) **Security Objectives**: Security objectives describe what needs to be completed for the identified threats to be mitigated.
3) **Security Requirements**: Security requirements that the TOE type should meet for the security objectives to be considered fulfilled. Security requirements include:
    a. **Functional Requirements (SFRs)**: Address the specific security functions the TOE type must provide, such as encryption or access control.
    b. **Assurance Requirements (SARs)**: Define the evaluation rigor to ensure the TOE type's functionality is correctly implemented and tested.

3.1.2 Benefits of Protection Profiles

1) Standardization: Protection Profiles (PPs) provide a standardized set of security requirements for specific categories of Targets of Evaluation (TOE). This standardization ensures that similar TOE evaluated against the same PP meet consistent security criteria. This will facilitate comparability and interoperability.
2) Efficiency in evaluation: PPs define common security requirements, which streamline the evaluation process for TOE of the same category. Therefore, reducing the time and resources needed for individual TOE evaluation, because similar TOE can use the same set of requirements during evaluation.
3) Independent certification of PPs: New PPs can be certified independently, prior to the certification of a TOE. This means that the security requirements are defined and evaluated beforehand, creating a standardized and trusted baseline. By certifying PPs in advance, the overall certification process for TOE becomes more efficient and reliable, as the security requirements have already been validated.
4) Support for market confidence: By providing a clear framework for security requirements, PPs help build confidence among users and stakeholders regarding the security level of a certified TOE.
5) Global recognition: PPs are recognized under the Common Criteria framework, that is an international standard. Therefore, promoting international trade and cooperation in cyber security.

3.2 Security Targets

Security Targets (STs) are similarly recognized internationally under the Common Criteria framework, to Protection Profiles (PPs). While PPs define a standardized set of security requirements for a specific type of Targets of Evaluation (TOE), STs define specific security requirements for an individual TOE under evaluation. For example, a ST could describe the security requirements for the MinuteGap v18.5 Firewall, whereas a PP would refer to firewalls in general.

A ST outlines how the TOE meets the requirements; whenever necessary, it will reference the applicable PP, but the final version of the document will provide additional details that are unique to the TOE. The primary goal of STs is to demonstrate how a specific TOE fulfils the necessary security criteria, facilitating a thorough and consistent evaluation process. If the TOE satisfies the requirements outlined in the ST, it can achieve certification, demonstrating its compliance with the specified security standards.

3.2.1 Components of Security Targets

1) **Security Problem Definition**: Similar to Protection Profiles (PPs), Security Problem Definition describes the security environment of the Security Target (ST) and includes threats, assumptions, and organizational security policies. However, it is tailored to the context of a specific Targets of Evaluation (TOE).
2) **Security Objectives**: Security objectives describe what needs to be completed in order for the identified threats to be mitigated, focusing on the specific TOE being evaluated.

3) **Security Requirements**: Security requirements that the specific TOE should meet in order for the security objectives to be considered fulfilled. Security requirements include:
   a. **Functional Requirements (SFRs)**: Address the specific security functions the TOE must provide, such as encryption or access control.
   b. **Assurance Requirements (SARs)**: Define the evaluation rigor to ensure the TOE's functionality is correctly implemented and tested.

3.2.2 Benefits of Security Targets

The benefits of Security Targets (STs) and Protection Profiles (PPs) are essentially the same, with the primary difference being their focus. While both provide standardization, efficiency in evaluation, risk management, and support for certification, STs focus on the specific requirements of a specific TOE. In contrast, PPs define a reusable set of security requirements for a broader category or TOE type. Essentially, STs are tailored to a specific TOEt's needs, while PPs offer a standardized baseline that can be applied across similar TOE within a category.

3.3 Evaluation Assurance Levels

In the context of Common Criteria, Evaluation Assurance Levels (EALs) are used for the evaluation of the security properties of Targets of Evaluation (TOE). EALs provide a standardised way to measure the assurance that the TOE meets its security requirements mentioned in the respective Protection Profile (PP) or Security Target (ST). EALs are a set of predefined levels that indicate the depth and rigor of the evaluation process needs to go into and each level corresponds to a specific collection of evaluation activities and assurance requirements.

EALs serve as a means of assuring customers and users with a clear understanding of the assurance level they can expect from a certified TOE. The higher the level, the more thorough the evaluation process, indicating greater confidence in the TOE’s security.

3.3.1 Levels of Evaluation Assurance Levels

The Common Criteria (CC) defines several Evaluation Assurance Levels (EALs), ranging from level 1 through 7, that are mentioned as EAL1 to EAL7 respectively. In more detail they are the following:

Table 1: Evaluation Assurance Levels

EAL Level	Name	Description	Example Use Case
EAL1	Functionally tested	Basic testing of the TOE's functionality	A consumer-grade IoT device, such as a smart light bulb
EAL2	Structurally tested	More rigorous testing, including examination of the design and implementation	A secure USB flash drive for personal use

EAL3	Methodically tested and checked	Comprehensive testing and analysis of the TOE's security features	A network firewall for small businesses
EAL4	Methodically designed, tested, and reviewed	Involves a thorough design and testing process, including independent review	An enterprise-grade secure operating system, such as Windows Server OS or Red Hat Enterprise Linux
EAL5	Semi-formally designed and tested	Requires formal methods for design and testing, providing a higher level of assurance	A smart card used for secure payments (e.g., EMV payment systems)
EAL6	Semi-formally verified design and tested	Involves rigorous verification of the design and testing processes	A hardware security module (HSM) used for managing cryptographic keys in banking systems
EAL7	Formally verified design and tested	The highest level of assurance, requiring formal proofs of security properties	A cryptographic module for military-grade communication systems

3.4 Evaluation Methodology

The evaluation methodology provides a systematic approach to assess the security functionality and assurance of Targets of Evaluation (TOE). This methodology ensures a standardized, rigorous evaluation conducted by CBs, providing confidence in the security and reliability of the TOE. It aims to ensure that the products or services meet their respective security target specifications and that they comply with the specified Evaluation Assurance Levels (EALs). The core benefit of using the evaluation methodology for certifying TOE is that it promotes harmonization across different evaluation bodies and countries, facilitating international recognition of the certification. This is of particular importance for international trade and collaboration in the cybersecurity field.

The final step of the evaluation methodology is a certification report that documents the evaluation process, findings, and results. This report serves as the foundation for issuing a Common Criteria (CC) certificate, which verifies the TOE’s compliance with the specified security requirements.

3.4.1 Components of the Evaluation Methodology

The evaluation methodology typically includes several key components:

1) **Security Target (ST)**: The evaluation begins with the review of the ST, which outlines the security requirements and objectives for the TOE.
2) **Protection Profiles (PP)**: If applicable, the evaluation may reference PP that define common security requirements for a TOE type.
3) **Evaluation Assurance Levels (EALs)**: The methodology specifies the EAL that the TOE is aiming to achieve, which dictates the depth and rigor of the evaluation process.
4) **Evaluation Activities**: The methodology outlines specific activities that evaluators must perform, including:
    a. **Document Review**: Evaluators review the TOE’s documentation, including design specifications, user manuals, and security policies.

b. **Testing**: Evaluators conduct tests to verify that the TOE meets its security functional requirements. This may include functional testing, penetration testing, and vulnerability assessments.
c. **Analysis**: Evaluators analyse the results of the testing and review to determine whether the TOE meets the security requirements outlined in the ST.
d. **Independent Review**: For higher EALs, an independent review of the evaluation process and results may be required to ensure objectivity and thoroughness.

3.4.2 Common Evaluation Methodology

The Common Evaluation Methodology (CEM) is a key document that provides detailed guidance on how evaluation should be conducted under the Common Criteria (CC) framework. It provides guidance during the evaluation process, including the steps that should be followed, the evaluation activities, as well as the assurance requirements that need to be met. A more detailed explanation of the CEM will be provided in a later section.

3.5 Assurance Components

Assurance components are specific criteria that define the level of confidence in the security functionality of a Target of Evaluation (TOE). They are categorized into two main families: Security Functional Requirements (SFRs) and Security Assurance Requirements (SARs). The assurance components provide a means for evaluating the effectiveness of the security measures implemented in a product or service. As previously mentioned, the Common Criteria (CC) uses Evaluation Assurance Levels (EALs) to classify these components, with higher EALs indicating the need for a greater depth of evaluation and assurance. These components are used by the CBs in order to assess the TOE’s resistance to vulnerabilities and its overall security posture, ensuring that the chosen assurance level is appropriate.

3.5.1 Security Functional Requirements

Security Functional Requirements (SFRs) are a set of security features that an IT product or service must provide in order to meet its security objectives. These requirements are derived from the Security Target (ST) that describe this specific Target of Evaluation (TOE) and are categorized into various categories. The SFRs categories in the Common Criteria (CC) are organized into classes that represent broad categories of security functionality. Each class is further divided into families which group together related security functions within a specific domain. For example, the FAU: Security Audit class includes families such as FAU_GEN (Security Audit Data Generation) and FAU_STG (Security Audit Event Storage). This structured approach facilitates the precise specification of security features required for the TOE. For detailed information about the families within each class of SFRs, please refer to Appendix I.

3.5.2 Security Assurance Requirements

The Security Assurance Requirements (SARs) safeguard and support the implementation of Security Functional Requirements (SFRs) by ensuring their correctness, completeness, and resilience against security threats. While SFRs define the security behaviour or capabilities a Target of Evaluation (TOE) should meet, SARs focus on providing confidence in the quality and integrity of those implementations through rigorous evaluation and verification. They do so by requiring systematic testing, design review, and analysis. This proactive approach ensures that vulnerabilities are mitigated on a regular basis and any residual risks are identified and managed appropriately.

Similarly to SFRs, the SARs categories in the Common Criteria (CC) are also organized into classes, which are then further divided into families. For example, the APE: Protection Profile (PP) evaluation class includes families such as APE_SPD (Security problem definition) and APE_REQ (Security requirements). This structured approach facilitates the precise specification of security features required for the TOE. For detailed information about the families within each class of SARs, please refer to Appendix II.

3.6 Technical Domains

In the context of Common Criteria (CC), Technical Domains are broader categories or frameworks that group Information Technology (IT) products or services with similar security functionalities, risks, and evaluation needs. They provide a general structure for evaluations, including specific methodologies, tools, and state-of-the-art requirements applicable to a range of products. One example of a Technical Domain could be the smart cards.

Not to be confused with Target of Evaluation (TOE) types, which are more specific classifications of the individual IT product or service types within those technical domains. While Technical Domains organize products at a high level by grouping them into broad categories, TOE types focus on classes of products with distinct security features and evaluation criteria. In the example of smart cards, the TOE types of this particular technical domain could be smart cards used for secure authentication, smart cards for payment systems, or cryptographic tokens with secure key storage.

3.7 Certification Bodies

Certification Bodies (CBs), as defined in the Common Criteria (CC) are conformity assessment organizations responsible for conducting evaluations and issuing certifications for Information Technology (IT) products or services based on the CC framework. The role of is to ensure the Targets of Evaluation (TOE) meet the specified security functional and assurance requirements as described in the CC framework, providing a layer of confidence to users and stakeholders regarding the security level or the evaluated product or service.

CBs must be accredited by national authorities or recognized organizations to ensure their competence and impartiality in conducting evaluations. This accreditation process helps maintain the integrity and reliability of the certification process. CBs operate in accordance with the CC and relevant regulations, ensuring that their evaluation methods and practices align with international standards. This compliance is essential for the mutual recognition of certifications across different countries and regions.

CBs often work in conjunction with IT Security Evaluation Facilities (ITSEFs), which perform the actual evaluations of the products. CBs and ITSEFs play complementary roles in the CC certification process. ITSEFs are accredited, independent laboratories tasked with performing the detailed technical evaluation of the TOE. Once the ITSEF completes its evaluation, it compiles a detailed evaluation report summarizing its findings. This report includes evidence provided by the product developer, such as design documentation, test plans, and results. It also contains the ITSEF's conclusions regarding the product's compliance with the security functional and assurance requirements. Lastly, the CB reviews the findings and evidence provided by the ITSEF before issuing the final certification. This collaborative process ensures a separation of duties, with ITSEFs focusing on technical evaluation and CBs ensuring the integrity and impartiality of the certification process. Together, they provide assurance that certified products meet stringent security standards.

3.7.1 Evaluation Process

CBs oversee the evaluation process, conducted by accredited evaluation facilities, commonly known as laboratories. This process typically includes:

1) Reviewing the Security Target (ST), which outlines the security claims of the product.
2) Verifying that the product meets the defined Protection Profile (PP), if applicable.
3) Evaluating evidence provided by the developer, such as design documentation, test results, and vulnerability analyses.
4) Conducting independent testing to confirm that the product behaves as claimed.
5) CBs ensure that evaluations adhere to the standards and methodologies specified in the Common Criteria Evaluation and Validation Scheme (CCEVS).

Upon successful evaluation, CBs issue Common Criteria certificates, which indicate the Evaluation Assurance Level (EAL) achieved by the product. The certification reflects the degree of confidence in the product's security properties based on the rigor of the evaluation process.

4. COMMON EVALUATION METHODOLOGY THE GROUNDWORK FOR EUCC

Common Evaluation Methodology (CEM) refers to the Common Methodology for Information Technology Security Evaluation, as set out in the ISO/IEC standard ISO/IEC 18045. The primary purpose of the ISO/IEC 18045 standard is to define the minimum actions that evaluators must perform to conduct a Common Criteria (CC) evaluation. The CEM serves as a foundational component of the Common Criteria framework, providing a standardized and systematic approach for evaluating the security of Target of Evaluations (TOE). CEM aims to ensure that evaluators have the necessary guidance to assess the security of IT products and systems accurately and reliably. This includes the evaluation of evidence, the performance of evaluation sub-activities, and the assignment of verdicts based on the evaluation results.

Within the context of the EUCC scheme, the CEM is adapted to align with the specific requirements and objectives of the European market. This ensures that evaluations conducted under the EUCC are both rigorous and consistent with EU regulations and directives. While the Common Criteria and CEM have a global scope, the tailored application of the CEM under the EUCC scheme guarantees that ICT TOEs not only meet international security standards but also address the unique security needs and legal frameworks of the EU. This adaptation reinforces trust in ICT products certified for the European market while maintaining compatibility with the broader international framework.

4.1 Evaluation Process

The evaluation process overview in the Common Evaluation Methodology (CEM) includes several critical elements related to roles, responsibilities, relationships, and the general evaluation model.

4.1.1 Roles and Responsibilities

The general model defines the following roles: sponsor, developer, evaluator and evaluation authority:

1) **Sponsors**: The one who is responsible for requesting and supporting an evaluation.
2) **Developers**: Those who produce the target of evaluation (TOE) being evaluated and are also responsible for providing the required evidence for the evaluation.
3) **Evaluator**: The evaluator performs the evaluation tasks required in the context of an evaluation: the evaluator receives the evaluation evidence from the developer on behalf of the sponsor or directly from the sponsor, performs the evaluation sub-activities and provides the results of the evaluation assessment to the evaluation authority.
4) **Evaluation Authority**: The evaluation authority establishes and maintains the scheme, monitors the evaluation conducted by the evaluator, and issues certification/validation reports as well as certificates based on the evaluation results provided by the evaluator.

For an evaluation to be conducted without influence, the roles of evaluator and evaluation authority need to be fulfilled by deferent entities. The roles of developer and sponsor can be satisfied by a single entity.

4.1.2 General Evaluation Model

The evaluation process consists of the evaluator performing the evaluation input task, the evaluation output task and the evaluation sub-activities.

1) **Evaluation Input Task**: During this task, the evaluators ensure that have access to the correct adequacy protected version of all necessary evaluation evidence. This task is primarily the responsibility of the sponsor, although much of the evidence is typically produced by the developer on the sponsor's behalf. Evaluation evidence may include design documents, source code or any other related documentation.
2) **Evaluation Evidence Sub-Task**: This task describes multiple activities that the evaluator should perform.
    a. Management and organization of the evaluation evidence collected during the previous task.
    b. Configuration control that allows to identify and locate each item of evidence and verify the specific versions in their possession.
    c. Disposal of evaluation evidence at the conclusion of the evaluation, which may involve returning, archiving, or destroying the materials.
    d. The evidence may have sensitive information and therefore need to be handled with confidentiality in mind, necessitating strict controls on the handling and storage of evaluation evidence.
3) **Evaluation Output Task**: The primary objective of this task is to produce comprehensive reports that include:
    a. **Observation Report (OR)**: The OR is a document that captures specific observations made during the evaluation process, including any issues or clarifications needed, along with their severity and the responsible parties for resolution.
    b. Evaluation Technical Report (ETR): The ETR is a comprehensive report that presents the technical justification for the evaluation verdicts, detailing the evaluation findings, conclusions, and recommendations related to the TOE.

   These reports serve as formal records of the evaluation process and its outcomes, providing essential information to the evaluation authority and stakeholders

4.1.3 Evaluation Verdict

The evaluation verdict represents the conclusion of the evaluation process and is determined based on the evidence and activities performed during the evaluation. In other words, the evaluation verdict is the logical conclusion of the activities described in the General Evaluation Model. The verdict is assigned to the most granular Common Criteria (CC) structure, the evaluation action element and is assigned after performing the corresponding evaluation methodology action and its constituent work units. Therefore, each evaluation action element gets its own verdict (pass, fail or inconclusive).

Multiple evaluation action elements are grouped into assurance components, and for an assurance component to pass it is mandatory all the included evaluation action elements to not have failed. Then all assurance components are grouped into assurance components, and if an assurance component within the class fails, the whole assurance class is marked as failed.

The overall evaluation result aggregates all assurance classes, which all need to be passed for the overall evaluation to be marked as passed.

As previously mentioned, there are three possible stated for a verdict:

1) **Pass verdict**: A pass verdict is assigned when the evaluator determines that the evaluated component meets all the required criteria. Specifically, the conditions for a pass are:
    a. The work units associated with the evaluation methodology action are fully completed.
    b. All evaluation evidence is coherent, meaning it is understandable and usable without requiring additional clarification.
    c. There are no obvious inconsistencies in the evidence. Obvious inconsistencies refer to errors that the evaluator identifies naturally while performing their tasks, without needing to conduct a full-scale consistency analysis across all evidence.
2) **Fail verdict**: A fail verdict is given when the evaluator identifies that:
    a. The evaluated component does not meet the required criteria.
    b. The evidence provided is incoherent or incomplete, making it difficult or impossible for the evaluator to complete the work units.
    c. An obvious inconsistency in the evidence has been found during the evaluation process.
3) **Inconclusive verdict**: Initially, all verdicts are considered inconclusive until the evaluator has completed their analysis and made a definitive determination of pass or fail. As mentioned above, given that even one evaluator action element in an assurance component is marked as fail, the entire assurance component is marked fail. This means the remaining action elements within that component don't need to be further analyzed or assigned a verdict, in that case they can remain inconclusive because the component's outcome is already decided. This is the only case the verdict can remain inconclusive.

4.2 Classes of Evaluation

The Common Evaluation Methodology (CEM), Organizes the evaluation process into distinct classes. Each class assesses a different aspect of a target of evaluation (TOE) and corresponds to a specific area during the security evaluation. These classes are aligned with the structure and requirements defined in the Security Assurance Requirements (SARs) in the context of Common Criteria (CC) framework. The classes of evaluation are:

1) **APE**: Protection Profile (PP) evaluation
2) **ACE**: Protection Profile Configuration evaluation
3) **ASE**: Security Target (ST) Evaluation
4) **ADV**: Development
5) **AGD**: Guidance Document
6) **ALC**: Life-cycle Support
7) **ATE**: Tests
8) **AVA**: Vulnerability Assessment
9) **ACO**: Composition

Using these predefined classes, CEM achieves holistic evaluation of the TOE, addressing all distinct aspects of its security posture during the evaluation. In this way CEM ensures that the TOE meets the required assurance level and fulfills its security objectives effectively.

By breaking down the evaluation into smaller, more manageable parts, the CEM promotes consistency, repeatability and a thorough review process.

5. CONCLUSIONS

The EU Cybersecurity Certification Scheme on Common Criteria (EUCC) can be seen as a significant step toward the creation of a standardized and robust certification process for ICT products inside the European Union. By leveraging the Common Criteria framework, the EUCC ensures that products meet predefined specific security requirements, thereby fostering trust among users and businesses.

Despite its advantages, the adoption of the EUCC faces challenges, including industry adaptation, stakeholder coordination, and potentially emerging cybersecurity threats. The need for continuous updates and alignment with state-of-the-arts technologies remains a critical aspect of the scheme’s long-term effectiveness. Additionally, the successful integration of the EUCC with global cybersecurity frameworks will be essential to ensuring international cooperation and recognition.

In conclusion, while the EUCC is a major advancement in cybersecurity certification, its long-term success depends on the commitment of regulators, industry participants, and policymakers to refine and adapt the scheme during upcoming technological advancements. Moving forward, continued stakeholder engagement, regulatory oversight, and technological innovation will be essential to strengthening Europe’s cybersecurity resilience in an increasingly interconnected digital landscape.

6. ABBREVIATIONS – INITIALISMS – ACRONYMS

AVA_VAN	Assurance Family “Vulnerability Analysis”
CERT	Computer Emergency Response Team
CB	Certification Bodies
CC	Common Criteria
CEM	Common Evaluation Methodology
CVE	Common Vulnerabilities and Exposures
CAB	Conformity Assessment Body
CSA	Cybersecurity Act
CP	Composite Product
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
IAR	Impact Analysis Report
MSA	Market Surveillance Authority
NCCA	National Cybersecurity Certification Authority
PP	Protection Profile
SAR	Security Assurance Requirements
SFR	Security Functional Requirements
ST	Security Target
SOG-IS	Security Officials Group Information Systems Security
SOG-IS MRA	SOG-IS Mutual Recognition Agreement
TD	Technical Domain
TOE	Target of Evaluation
ITSEF	Testing Laboratory / Evaluation Facility

7. APPENDIX I

The Common Criteria CC:2022 Part 2 Revision 1 was published in November 2022 by Common Criteria Recognition Arrangement (CCRA), with contributions from several national governmental organizations, including several EU countries. Part 2: Security functional components of the CC focuses on Security Functional Requirements (SFRs), providing detailed criteria for defining specific security behaviors in IT products and services.

Table 2: Overview of CC:2022 Security Functional Requirements Families

Class Name	Family Short Name	Description
FAU: Security Audit	FAU_ARP	Security audit automatic response
	FAU_GEN	Security audit data generation
	FAU_SAA	Security audit analysis
	FAU_SAR	Security audit review
	FAU_SEL	Security audit event selection
	FAU_STG	Security audit event storage
FCO: Communication	FCO_NRO	Non-repudiation of origin
	FCO_NRR	Non-repudiation of receipt
FCS: Cryptographic Support	FCS_CKM	Cryptographic key management
	FCS_COP	Cryptographic operation
	FCS_RBG	Random bit generation
	FCS_RNG	Generation of random numbers
FDP: User Data Protection	FDP_ACC	Access control policy
	FDP_ACF	Access control functions
	FDP_DAU	Data authentication
	FDP_ETC	Export from the TOE
	FDP_IFC	Information flow control policy
	FDP_IFF	Information flow control functions
	FDP_IRC	Information retention control
	FDP_ITC	Import from outside the TOE
	FDP_ITT	Internal TOE transfer
	FDP_RIP	Residual information protection
	FDP_ROL	Rollback
	FDP_SDC	Stored data confidentiality
	FDP_SDI	Stored data integrity
	FDP_UCT	Inter-TSF user data confidentiality transfer protection
	FDP_UIT	Inter-TSF user data integrity transfer protection
FIA: Identification and Authentication	FIA_AFL	Authentication failures
	FIA_API	Authentication proof of identity
	FIA_ATD	User attribute definition
	FIA_SOS	Specification of secrets
	FIA_UAU	User authentication
	FIA_UID	User identification
	FIA_USB	User-subject binding
	FMT_LIM	Limited capabilities and availability

FMT: Security Management	FMT_MOF	Management of functions in TSF
	FMT_MSA	Management of security attributes
	FMT_MTD	Management of TSF data
	FMT_REV	Revocation
	FMT_SAE	Security attribute expiration
	FMT_SMF	Specification of Management Functions
	FMT_SMR	Security management roles
FPR: Privacy	FPR_ANO	Anonymity
	FPR_PSE	Pseudonymity
	FPR_UNL	Unlikability
	FPR_UNO	Unobservability
FPT: Protection of the TSF	FPT_EMS	TOE emanation
	FPT_FLS	Fail secure
	FPT_INI	TSF initialization
	FPT_ITA	Availability of exported TSF data
	FPT_ITC	Confidentiality of exported TSF data
	FPT_ITI	Integrity of exported TSF data
	FPT_ITT	Internal TOE TSF data transfer
	FPT_PHP	TSF physical protection
	FPT_RCV	Trusted recovery
	FPT_RPL	Replay detection
	FPT_SSP	State synchrony protocol
	FPT_STM	Time stamps
	FPT_TDC	Inter-TSF TSF data consistency
	FPT_TEE	Testing of external entities
	FPT_TRC	Internal TOE TSF data replication consistency
	FPT_TST	TSF self-test
FRU: Resource Utilization	FRU_FLT	Fault tolerance
	FRU_PRS	Priority of service
	FRU_RSA	Resource allocation
FTA: TOE Access	FTA_LSA	Limitation on scope of selectable attributes
	FTA_MCS	Limitation on multiple concurrent sessions
	FTA_SSL	Session locking and termination
	FTA_TAB	TOE access banners
	FTA_TAH	TOE access history
	FTA_TSE	TOE session establishment
FTP: Trusted Path/Channels	FTP_ITC	Inter-TSF trusted channel
	FTP_PRO	Trusted channel protocol
	FTP_TRP	Trusted path

8. APPENDIX II

The Common Criteria CC:2022 Part 3 Revision 1 was published in November 2022 by Common Criteria Recognition Arrangement (CCRA), with contributions from several national governmental organizations, including several EU countries. Part 3: Security assurance components of the CC focuses on Security Assurance Requirements (SARs), providing detailed criteria for evaluating the assurance levels of IT products and services.

Table 3: Overview of CC:2022 Security Assurance Requirements Families

Class Name	Family Short Name	Description
APE: Protection Profile (PP) evaluation	APE_INT	PP introduction
	APE_CCL	Conformance claims
	APE_SPD	Security problem definition
	APE_OBJ	Security objectives
	APE_ECD	Extended components definition
	APE_REQ	Security requirements
ACE: Protection Profile Configuration evaluation	ACE_INT	PP-Module introduction
	ACE_CCL	PP-Module conformance claims
	ACE_SPD	PP-Module security problem definition
	ACE_OBJ	PP-Module security objectives
	ACE_ECD	PP-Module extended components definition
	ACE_REQ	PP-Module security requirements
	ACE_MCO	PP-Module consistency
	ACE_CCO	PP-Configuration consistency
ASE: Security Target (ST) Evaluation	ASE_INT	ST introduction
	ASE_CCL	Conformance claims
	ASE_SPD	Security problem definition
	ASE_OBJ	Security objectives
	ASE_ECD	Extended components definition
	ASE_REQ	Security requirements
	ASE_TSS	TOE summary specification
	ASE_COMP	Consistency of composite product ST
ADV: Development	ADV_ARC	Security architecture
	ADV_FSP	Functional specification
	ADV_IMP	Implementation representation
	ADV_INT	TSF internals
	ADV_SPM	Security policy modelling
	ADV_TDS	TOE design
	ADV_COMP	Composite design compliance
AGD: Guidance Document	AGD_OPE	Operational user guidance
	AGD_PRE	Preoperative procedures
ALC: Life-cycle Support	ALC_CMC	CM capabilities
	ALC_CMS	CM scope
	ALC_DEL	Delivery
	ALC_DVS	Developer environment security
	ALC_FLR	Flaw remediation

	ALC_LCD	Development life-cycle definition
	ALC_TDA	TOE development artefacts
	ALC_TAT	Tools and techniques
	ALC_COMP	Integration of composition parts and consistency check of delivery procedures
ATE: Tests	ATE_COV	Coverage
	ATE_DPT	Depth
	ATE_FUN	Functional tests
	ATE_IND	Independent testing
	ATE_COMP	Composite functional testing
AVA: Vulnerability Assessment	AVA_VAN	Vulnerability analysis
	AVA_COMP	Composite vulnerability assessment
ACO: Composition	ACO_COR	Composition rationale
	ACO_DEV	Development evidence
	ACO_REL	Reliance of development component
	ACO_CTT	Composed TOE testing
	ACO_VUL	Composition vulnerability analysis

9. BIBLIOGRAPHY

[1] ENISA, "Cybersecurity Certification: EUCC, a candidate cybersecurity certification scheme to serve as a successor to the existing SOG-IS", Version 1.0, European Union Agency for Cybersecurity, July 2020.

[2] European Commission, "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)", 2024.

[3] Common Criteria, "Common Criteria for Information Technology Security Evaluation, Part 2: Security functional components," CC:2022 Revision 1, CCMB-2022-11-002, November 2022.

[4] Common Criteria, "Common Criteria for Information Technology Security Evaluation, Part 3: Security assurance components", CC:2022 Revision 1, CCMB-2022-11-003, November 2022.

[5] Common Criteria, "Common Methodology for Information Technology Security Evaluation: Evaluation methodology", CEM:2022 Revision 1, CCMB-2022-11-006, November 2022.

[6] Management Committee, “Mutual Recognition Agreement of Information Technology Security Evaluation Certificates”, Version 3.0, Final Version, January 8th, 2010.

[7] ENISA, "Minimum ITSEF requirements for security evaluations of smart cards and similar devices", Version 1.1, European Union Agency for Cybersecurity, October 2023.

[8] ENISA, "Minimum Site Security Requirements", Version 1.1, European Union Agency for Cybersecurity, October 2023.

[9] ENISA, "Application of Common Criteria to integrated circuits", Version 1.1, European Union Agency for Cybersecurity, October 2023.

[10] ENISA, "Security Architecture Requirements for Smart Cards and Similar Devices", Version 1.1, European Union Agency for Cybersecurity, October 2023.

[11] ENISA, "Certification of ‘open’ smart card products", Version 1.1, European Union Agency for Cybersecurity, October 2023.

[12] ENISA, "Composite product evaluation for smart cards and similar devices", Version 1.1, European Union Agency for Cybersecurity, October 2023.

[13] ENISA, "Application of Attack Potential Smartcards", Version 1.1, European Union Agency for Cybersecurity, August 2023.

[14] ENISA, "Minimum ITSEF requirements for security evaluations of Hardware devices with security boxes", Version 1.1, European Union Agency for Cybersecurity, October 2023.

[15] ENISA, "Application of attack potential to hardware devices with security boxes", Version 1.1, European Union Agency for Cybersecurity, October 2023.