EUROPEAN UNION AGENCY
FOR CYBERSECURITY

EUCC SCHEME

STATE-OF-THE-ART DOCUMENT

Composite product evaluation and certification for CC: 2022

Version 1, February 2025

DOCUMENT HISTORY

Date	Version	Modification	Author's comments
October 2024	V1 draft1	Creation	Based on JIL-Composite-product-evaluation-for-Smart-Cards-and-similar-devices-v1.6. (https://sogis.eu/documents/cc/domains/sc/JIL-Composite-product-evaluation-for-Smart-Cards-and-similar-devices-v1.6.pdf)
February 2025	V1	Version based on EUCC maintenance subgroup review	Endorsed for publication on 11/03/2025 by the ECCG

LEGAL NOTICE

LEGAL NOTICE

This publication is a state-of-the-art document as defined in Article 2 point 14 of Commission Implementing Regulation (EU) 2024/482.

This document is established and endorsed by the European Cybersecurity Certification Group (ECCG) in accordance with Article 48 paragraphs 2 and 3 of Commission Implementing Regulation (EU) 2024/482.

This document shall be updated whenever needed to reflect the developments and best practices in the field of composite evaluations. Updates of this document shall be submitted to the ECCG for endorsement.

This document shall be read in conjunction with Regulation (EU) 2019/881, the Commission Implementing Regulation (EU) 2024/482, its annexes, and where applicable supporting documentation that is made available.

This document is made publicly accessible through the EU cybersecurity certification website and is free of charge.

ENISA is not responsible or liable for the use of the content of this document. Neither ENISA nor any person acting on its behalf or on behalf of the maintenance of the scheme is responsible for the use that might be made of the information contained in this publication.

CONTACT

Feedback or questions related to this document can be sent via the European Union Cybersecurity Certification website (https://certification.enisa.europa.eu/index_en).

TABLE OF CONTENTS

1. INTRODUCTION

1.1 BACKGROUND

Originally the so-called composite evaluation approach was set up under the SOG-IS umbrella for products of type smart card and similar devices and their efficient security evaluation according to Common Criteria. This evaluation approach as outlined and specified in corresponding SOG-IS supporting documents was widely used and experienced for this product category in the past. To continue this success story in Common Criteria certification, the composite evaluation approach was with a slightly widened scope transferred to the Common Criteria standard, hereby at first incorporated into (CC) and (CEM).

A more detailed description of the overall concept of the composite evaluation approach with all its objectives, main structure and processes, benefits, issues, rules, specifics and constraints is available in (CC) part 1, sections 14.2.1, 14.3.3, 14.4 and 14.5. The composite evaluation technique defines specific action elements to be performed by the actors involved in the evaluation of the base component, as well as in the development of the dependent component and in the integration and evaluation of the composite product. Please take into account that the terminology used for the composite evaluation approach defined by SOG-IS changed from “platform Target of Evaluation (TOE)/product” to “base TOE/component” and from “application TOE/product” to “dependent TOE/component” in order to address the above mentioned slightly widened scope of the composite evaluation approach in the Common Criteria standard.

As experienced in the past, the concept of so-called ‘composed TOEs’ and their security evaluation according to the Common Criteria – refer to the specific assurance class ACO and the CAP packages for composed TOEs in (CC) part 1, (CC) part 3, (CC) part 5 and (CEM) – is not suitable for security evaluation of each and any specific product type, in particular not for usual security evaluation in the area of smart card and similar devices products. For the latter one, the composite evaluation approach is the more suitable one. In addition, please take into account that the concept of composite evaluation does not limit the evaluation regards the evaluation assurance level (EAL) and resistance against attacks, i.e., up to attack potential ‘high’, whereas the composed TOE evaluation approach using the ACO class and CAP packages is limited by resistance against attacks of attack potential ‘enhanced-basic’.

1.2 OBJECTIVE AND SCOPE

This state-of-the-art document as defined under Article 2 point 14 of Regulation (EU) 2024/482 is a supporting document under Implementing Regulation (EU) 2024/482 on establishing the Common Criteria-based cybersecurity certification scheme (EUCC).

The overall composite evaluation approach is described in (CC) part 1, sections 14.2.1 and 14.3.3. Additional aspects are outlined in (CC) part 1, sections 14.4 and 14.5. Corresponding security assurance requirements (SARs) for specific composite evaluation aspects are specified in (CC) part 3, sections 9.9, 10.8, 12.10, 13.6 and 14.4 and accompanied by composite evaluation-specific activities (composite evaluation work units) in (CEM), sections 12.10, 13.9, 15.10, 16.7 and 17.3.

The objective of this document is to address composite certification aspects that are relevant for scheme harmonisation, but are not or only partly covered by the Common Criteria and especially the aforementioned (CC) part 1, (CC) part 3 and (CEM) sections. Hence, the purpose of the present document is to identify all relevant aspects for the composite evaluation approach and technique as outlined in the CC/CEM and to provide additional information, requirements and rules for composite certification procedures.

The composite evaluation approach as described in (CC) part 1, section 14.3.3 can be applied in principle to any secure IT product where an independently evaluated component is part of a final composite product to be evaluated. The composite evaluation approach addresses in particular TOEs that are of the type belonging to the technical domain “Smart Cards and similar devices”. However, the composite evaluation approach is not restricted to smart cards and similar devices only. In this sense the present document is in the same way intended for composite

certification aspects regarding the general composite evaluation approach addressed in (CC) and (CEM). Where applicable, specific aspects for smart cards and similar devices are considered in the following sections.

Specific examples and descriptions in (CC) part 1, section 14.3.3 illustrate the application of the composite evaluation approach in the area of smart cards and similar devices.

1.3 NORMATIVE REFERENCES

Regulations

Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act)

Implementing Regulation (EU) 2024/482 on establishing the Common Criteria-based cybersecurity certification scheme (EUCC)[1], as amended by Implementing Regulation 2024/3144

Standards

Unless otherwise specified, the versions of the Common Criteria and Common Evaluation Methodology standards defined in Article 2 of the EUCC scheme apply.

EUCC state-of-the-art documents[2]

Unless otherwise specified, the latest version of referenced state-of-the-art documents applies:

- Application of attack potential to smartcards and similar devices
- Composite product evaluation for smart cards and similar devices for CC 3.1

1.4 ACRONYMS AND DEFINITIONS

1.4.1 Acronyms

CAB	Conformity assessment body
CB	Certification body
CC	Common Criteria for Information Technology Security Evaluation as defined the EUCC
CEM	Common Methodology for Information Technology Security Evaluation as defined the EUCC
CSA	Cybersecurity Act
EAL	Evaluation Assurance Level
EC	European Commission
ENISA	European Union Agency for Cybersecurity
ETR	Evaluation technical report
EU	European Union
ICT	Information and communications technology
IEC	International Electrotechnical Commission
ISO	International Organisation for Standardisation
IT	Information technology
ITSEF	Information Technology Security Evaluation Facility
PP	Protection profile
SFR	Security functional requirement
SMEs	Small and medium enterprises
SOG-IS	Senior Officials Group – Information Systems Security
ST	Security target
TOE	Target of evaluation

[1] Available at http://data.europa.eu/eli/reg_impl/2024/482/oj
[2] Available at https://certification.enisa.europa.eu/certification-library/eucc-certification-scheme_en

TS Technical specification
TSFI TOE security function interfaces

1.4.2 Definitions

The definitions used under Article 2 of Regulation (EU) 2019/881 (Cybersecurity Act) and under Article 2 of the Implementing Regulation (EU) 2024/482 apply to this document. The following definitions also apply to this document.

Definitions and terminology used in the framework of the composite evaluation approach are additionally provided in (CC) part 1, sections 3 and 14.3.3.

Throughout the present document the terms “composite evaluation” and “composite product evaluation” are equivalently used, the same holds for the terms “composite certification” and “composite product certification” and further on for any similar expressions.

Due to specific requirements or constraints respectively concerning terminology used in (CC) and (CEM) (refer to (CC) part 1, section 3) the following mapping of terms will be used in the present document:

Table 1: Mapping of terms

Terms used in (CC) and (CEM)	Terms used in the present document
evaluation scheme	certification scheme
evaluator	evaluation body (ITSEF)
evaluation authority	certification body
report of the evaluation authority	certification report (including the related certificate) of the certification body

2. COMPOSITE EVALUATION

2.1 CONCEPT AND APPROACH

The overall composite evaluation approach with its objectives, main structure and processes, benefits, issues, rules, specifics and constraints is described in (CC) part 1, sections 14.2.1 and 14.3.3. Additional aspects are depicted in (CC) part 1, sections 14.4 and 14.5.

The role model for the composite evaluation approach is presented in (CC) part 1, section 14.3.3.4. The required information to be generated and exchanged among the different actors of that role model involved in a composite evaluation are addressed in (CC) part 1, sections 14.3.3.5, 14.3.3.6 and 14.3.3.7. In particular, Table 2 and Table 3 in (CC) part 1, section 14.3.3.5 provide a description which information that is of relevance for the composite evaluation approach has to be generated by whom and provided to the dependent component developer and the composite product evaluator or composite product evaluation authority (here: composite product certification body) respectively. Hereby, beyond the aforementioned requirements the required information shall be shared on a need-to-know basis according to the following table that complement the CC content:

Table 2: Specific deliveries between actors that complement the CC content

	Actors				
Documents/contributions to be provided to	**Composite product evaluation sponsor**	**Composite product integrator**	**Dependent component developer**	**Composite product evaluator**	**Composite product evaluation authority (certification body)**
Base component Security Target	No	No	Yes	Yes	Yes
Base component user guidance	No	Yes	Yes	Yes	Yes
Base component ETR for composite evaluation	No	No	No	Yes	Yes
Base component open samples3	No	No	No	Yes	No
Base component report of the base component evaluation authority (here: base component certification report)	Yes	Yes	Yes	Yes	Yes
Design compliance evidence	No	No	No	Yes	Yes
Composite configuration evidence	No	No	No	Yes	Yes
Delivery and acceptance procedures evidence	No	No	No	Yes	Yes

[3] Only relevant for composite evaluation in the area of smart cards and similar devices: if requested by the composite product evaluator as defined in state-of-the-art document APPLICATION OF ATTACK POTENTIAL TO SMARTCARDS AND SIMILAR DEVICES

The composite evaluation technique defines specific developer and evaluator action elements to be performed by the parties involved in the evaluation of the base component, as well as in the development of the dependent component and in the integration and evaluation of the composite product. These activities are addressed in more detail in the following section 5 of the present document.

2.2 ETR FOR COMPOSITE EVALUATION

To allow the evaluation of a composite product according to the composite evaluation approach, the composite evaluation technique requires the fulfilment of specific issues and actions, the generation of specific documentation and the exchange of that documentation among the different parties involved in the composite evaluation. Please refer to the details depicted in (CC) part 1, sections 14.3.3.5, 14.3.3.6 and 14.3.3.7.

Concerning the so-called Evaluation Technical Report (ETR) for composite evaluation (ETR_COMP), please refer to (CC) part 1, sections 14.3.3.6 and 14.3.3.7. Those sections provide detailed information on the role and objective of the ETR_COMP, surrounding procedures, exchange of the ETR_COMP, its validity regards re-use and an overview of its contents including explanatory information. In addition, as the ETR_COMP may contain intellectual property of the base component developer as well as of the base component evaluator, and also the base component evaluation authority (here: base component certification body) plays a role in its contents, at the minimum the document should be considered restricted. Furthermore, the ETR_COMP shall not include information affecting national security. A template for an ETR_COMP document for the technical domain “Smart Cards and similar devices” is given in Appendix 1 of this document.

2.3 COMPOSITE EVALUATION RULES AND ACTIVITIES ACCORDING TO CC

Security assurance requirements (SARs) for specific composite evaluation aspects are specified in (CC) part 3, sections 9.9, 10.8, 12.10, 13.6 and 14.4 and accompanied by corresponding composite evaluation activities and work units in (CEM), sections 12.10, 13.9, 15.10, 16.7 and 17.3. They are based on and correspond to the overall composite evaluation approach as described in (CC) part 1, sections 14.2.1, 14.3.3, 14.4 and 14.5.

In particular, composite evaluation-specific developer and evaluator action elements as well as related composite evaluation-specific evaluator activities and work units within the SAR families ASE_COMP, ADV_COMP, ALC_COMP, ATE_COMP and AVA_COMP are defined. They all are derived from the “usual” SAR classes ASE, ADV, ALC, ATE and AVA respectively and support in an efficient way the composite evaluation of a composite product. The SAR components ASE_COMP.1, ADV_COMP.1, ALC_COMP.1, ATE_COMP.1 and AVA_COMP.1 are relevant for composite evaluation and collected in the composite product assurance package “COMP” in (CC) part 5, section 6.

The SAR components of the composite product assurance package “COMP” address topics and issues as the evaluation of the composite product Security Target, the design compliance of the composite product’s base and dependent component, the compatibility check for delivery and acceptance procedures, the integration of the base and the dependent component resulting in the composite product, the composite product functional testing, and the composite product vulnerability analysis.

The COMP-related assurance requirements aim to give the composite product evaluator and the dependent component developer a precise guidance on which relevant aspects have to be described and assessed in the context of a composite evaluation and the tasks to be performed. Furthermore, this allows the composite product evaluation authority (here: composite product certification body) to check using the composite product ETR that the required (mandatory) tasks have completely and properly been performed.

The specific case of an already evaluated dependent component and possible reuse of already achieved evaluation results for the composite evaluation is addressed in (CC) part 1, section 14.3.3.5.

The current composite evaluation approach can be applied independently of the evaluation assurance level (EAL) for the composite product aimed. Where some evaluation activities are not applicable due to the EAL chosen, the related composite evaluation-specific tasks are also not expected to be applied.

2.4 VALIDITY OF REPORTS, CERTIFICATES AND ETR FOR COMPOSITE EVALUATION

Generic validity aspects and rules concerning the reports of evaluators and evaluation authorities (here, certification bodies) including the ETR for composite evaluation are addressed in (CC) part 1, section 14.3.3.7, but have to be supplemented accordingly for *composite* certification needs.

On base of (CC) part 1, section 14.3.3.7 with its NOTE 3, saying “Rules determining the validity and topicality of reports (here in particular the base component-related report of the base component evaluation authority (here: base component certification body) and the ETR for composite evaluation) are defined by the respective evaluation scheme and can be linked to a specifically defined validity period.”, the following (additional) rules and requirements for composite evaluation and certification of composite products hold:

The rules and requirements on validity aspects including topicality and relevance as depicted in (CC) part 1, section 14.3.3.7 (including NOTE 1 to 4) have to be applied. Hereby, validity rules and requirements concerning reports of evaluation authorities (here: certification reports of certification bodies) include the corresponding certificates that are issued by the respective evaluation authority (here: certification body) and that accompany the respective report.

To complement the CC the following rules are defined:

- The topicality for the ETR for composite evaluation in the technical domain “Smart Cards and similar devices” is determined by the state-of-the-art document APPLICATION OF ATTACK POTENTIAL TO SMARTCARDS AND SIMILAR DEVICES.
- The ETR for composite evaluation has a validity limit of a maximum of 18 months regarding re-use in composite evaluations. This 18-months rule concerns the submission of the evaluation report containing the full results of the vulnerability analysis and penetration testing within the composite evaluation procedure that is provided by the composite product evaluator to the composite product evaluation authority (here: composite product certification body). For chains of composite evaluations, the maximum validity period of 18 months is related to the eldest ETR for composite evaluation used in that chain of composite products and their evaluation.
- In continuation of (CC) part 1, section 14.3.3.7, Note 1: If the base component’s ETR for composite evaluation was issued less than 18 months ago before submission of the related composite evaluation tasks, but there was a major change in the state-of-the-art in performing relevant attacks on the base component (e.g. a major change in attack methods or attack ratings) then the composite product evaluation authority (here: composite product certification body) has the right to require a re-assessment of the base component focusing on the new attack (method, rating etc.). Specifically for the technical domain of smart cards and similar devices, this could also be imposed by major changes that are introduced in the state-of-the-art document APPLICATION OF ATTACK POTENTIAL TO SMARTCARDS AND SIMILAR DEVICES.

2.5 RULES, REQUIREMENTS AND HINTS FOR COMPOSITE CERTIFICATION

The following rules and requirements for composite certification of a composite product have to be applied.

Composite certification of a composite product requires a valid certificate and valid ETR for composite evaluation of the related base component.

For applying the composite evaluation technique, it is assumed that the level of assurance of the base component is equivalent or higher compared to the composite product evaluation level. Deviating cases have to be discussed within the CABs according to the rules defined in the EUCC Implementing Regulation.

The current composite evaluation approach can be applied independently of the evaluation assurance level (EAL) for the composite product aimed.

Composite evaluation and certification activities including evidence elements shall follow the rules depicted in this document including all requirements and descriptions incorporated via references to (CC) and (CEM). In particular, the information exchange and delivery rules for documentation as relevant for the composite evaluation approach described in section 5 shall be applied.

The composite product assurance package “COMP” in (CC) part 5, section 6 with its composite evaluation-specific assurance components ASE_COMP.1, ADV_COMP.1, ALC_COMP.1, ATE_COMP.1 and AVA_COMP.1 and in correspondence to that the SAR components specified in (CC) part 3, sections 9.9, 10.8, 12.10, 13.6 and 14.4 and evaluation activities and work units specified in (CEM), sections 12.10, 13.9, 15.10, 16.7 and 17.3 have to be carried out in the composite evaluation of the composite product.

For the composite product and its composite evaluation and certification, the composite product assurance package “COMP” in (CC) part 5, section 6 shall be claimed in the composite product Security Target.

Specifically, for the technical domain “Smart Cards and similar devices” the latest available version of the state-of-the-art document APPLICATION OF ATTACK POTENTIAL TO SMARTCARDS AND SIMILAR DEVICES has to be taken into account.

The validity rules, limits and requirements for re-use of reports, certificates and ETR for composite evaluation set up and provided by evaluators and evaluation authorities respectively -as outlined in section 6 of this document- have to be applied.

The ETR for composite evaluation related to a base component has to be covered by the base component’s evaluation and certification and to be depicted unambiguously in the related certification report (including its date and version). Application of the composite evaluation approach for the evaluation and certification of a composite product has to be outlined in the composite product’s certification report including a reference to the re-used base component’s ETR for composite evaluation. In the case of chains of composite evaluations, the entire list of re-used ETRs for composite evaluation has to be provided.

Assurance Continuity of composite certificates shall follow the general rules defined in the EUCC Implementing Regulation related to ASSURANCE CONTINUITY under consideration of composite evaluation aspects (including validity rules for re-use of evaluation activities and results). Hereby, for composite product changes the assessment of the changed composite product is always performed by the composite product evaluation authority (here: composite product certification body), but specifically in the case of a change of the related base component this assessment is performed based on the assessment of the changed base component by the base component evaluation authority (here: base component certification body).

A ANNEX

A.1 TEMPLATE FOR ETR FOR COMPOSITE EVALUATION

For the technical domain “Smart Cards and similar devices” a specific ETR for composite evaluation-document is available by the document template ETR FOR COMPOSITE EVALUATION TEMPLATE FOR THE TECHNICAL DOMAIN SMART CARDS AND SIMILAR DEVICES”. It is based on the general requirements as regards the contents of an ETR for composite evaluation as outlined in (CC) part 1, section 14.3.3.6.4 and the present document and provides additional specific requirements and explanatory information for application of the template for products of smart cards and similar devices type.

This guidance -document should be used as a template by the base component evaluator to issue the ETR for composite evaluation (ETR_COMP) for the technical domain “Smart Cards and similar devices”. For the purpose of this state-of-the-art document, note that the layout of the above-mentioned ETR template can be customized according to the practices of evaluation facilities company, but the contents and structure are mandatory.

For the ETR for composite evaluation-template for the technical domain “Smart Cards and similar devices”, the following mapping of terms has to be considered that reflects the usual terminology for products of smart cards and similar devices type:

Table 3: Mapping of terms for ETR for composite evaluation-template

Terms used in (CC)/(CEM) and the present document	Terms used in the ETR for composite evaluation template for the technical domain Smart Cards and similar devices
base component	platform
dependent component	application

Note: For future development of the present document on composite product evaluation and certification, further templates for the ETR for composite evaluation that address other composite product categories and their specifics may be elaborated and published for re-use.

A.2 BASE COMPONENT USER GUIDANCE REQUIREMENTS

Disclaimer: This section is not meant to be an appendix of an actual ETR for composite evaluation, but is included to support the base component developer in creation of user guidance requirements. These user guidance requirements have to be implemented by the dependent component developer in the dependent component to protect the TOE against certain attacks.

User guidance requirements that are provided to the dependent component developer must have the following properties:

1) It must be clear what the user has to do to protect the TOE.

2) It must be clear which attack (path or partial attack) the requirement is protecting from. The detail must be such that a dependent component developer will be able to perform a design compliance analysis. In other words, if a certain attack is not relevant for a dependent component the formulation must be such that a dependent component developer will recognise this.

A.3 MAPPING COMPOSITE PRODUCT EVALUATION TO COMMON CRITERIA (INFORMATIVE)

The preceding state-of-the-art document COMPOSITE PRODUCT EVALUATION FOR SMART CARDS AND SIMILAR DEVICES FOR CC 3.1 reflects the former SOG-IS supporting document for the composite evaluation approach. The following table provides a mapping of the content of this state-of-the art document to the sections of (CC) and (CEM). Please note that (CC) and (CEM) mainly cover composite evaluation related topics, whereas composite certification aspects are supplemented by the present document (refer to section 1.2).

Table 4: Mapping COMPOSITE PRODUCT EVALUATION FOR SMART CARDS AND SIMILAR DEVICES to Common Criteria

State-of-the-art document COMPOSITE PRODUCT EVALUATION FOR SMART CARDS AND SIMILAR DEVICES	(CC) and (CEM)
Section 2.1	(CC) part 1, section 14.3.3.1, 14.3.3.2, 14.3.3.3
Section 2.2	(CC) part 1, section 14.2.1, 14.3.3.4
Section 3.1	(CC) part 1, section 14.3.3.5
Section 3.2	(CC) part 1, section 14.3.3.5
Section 3.3	Refer to present document, section 2.5.
Section 3.4	(CC) part 1, section 14.3.3.5
Section 4.1	(CC) part 1, section 14.3.3.5
Section 4.2	(CC) part 1, section 14.3.3.5
Section 4.3	(CC) part 1, section 14.3.3.5
Section 4.4	(CC) part 1, section 14.3.3.5
Section 4.5	(CC) part 1, section 14.3.3.5
Section 4.6	(CC) part 1, section 14.3.3.5
Section 4.7	(CC) part 1, section 14.3.3.5
Section 5.1	(CC) part 1, section 14.3.3.6.1, 14.3.3.6.2
Section 5.2	(CC) part 1, section 14.3.3.6.1, 14.3.3.6.2 Refer to present document, section 2.2.
Section 5.3	(CC) part 1, section 14.3.3.6.3
Section 5.4	(CC) part 1, section 14.3.3.6.4
Section 6	(CC) part 1, section 14.3.3.7 Refer to present document, section 2.4 and 2.5.
Appendix 1	(CC) part 3, sections 9.9, 10.8, 12.10, 13.6 and 14.4 (CEM), sections 12.10, 13.9, 15.10, 16.7 and 17.3 (CC) part 1, section 14.4
Appendix 2	Refer to present document, Annex A1.
Appendix 3	Refer to present document, Annex A2.

ABOUT ENISA

The European Union Agency for Cybersecurity, ENISA, is the Union's agency dedicated to achieving a high common level of cybersecurity across Europe. Established in 2004 and strengthened by the EU Cybersecurity Act, the European Union Agency for Cybersecurity contributes to EU cyber policy, enhances the trustworthiness of ICT products, services and processes with cybersecurity certification schemes, cooperates with Member States and EU bodies, and helps Europe prepare for the cyber challenges of tomorrow. Through knowledge sharing, capacity building and awareness raising, the Agency works together with its key stakeholders to strengthen trust in the connected economy, to boost resilience of the Union's infrastructure, and, ultimately, to keep Europe's society and citizens digitally secure. More information about ENISA and its work can be found here: www.enisa.europa.eu.

ENISA
European Union Agency for Cybersecurity

Athens Office
Agamemnonos 14
Chalandri 15231, Attiki, Greece

Heraklion Office
95 Nikolaou Plastira
700 13 Vassilika Vouton, Heraklion, Greece

Brussels Office
Rue de la Loi 107
1049 Brussels, Belgium

enisa.europa.eu