Joint Interpretation Library

Composite product evaluation and certification

Subject:

Concept and methodology applicable to composite product evaluation and certification.

Version 1.6
April 2024

This page is intentionally left blank

Table of contents

Tables

1 Introduction

1.1 Background

1 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 (CC). This evaluation approach as outlined and specified in the JIL document "Composite product evaluation for Smart Cards and similar devices" (refer to [JIL COMP 1.5.1]) was widely used and experienced for this product category in the past. To continue this success story in CC certification, the composite evaluation approach was in slightly widened scope transferred to the CC standard, hereby at first incorporated into ISO/IEC 15408:2022 series and ISO/IEC 18045:2022 and subsequently and correspondingly taken over to CC:2022 ([CC]) and CEM:2022 ([CEM]).

2 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-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 in [JIL COMP 1.5.1] changed from "platform 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 CC standard.

3 As turned out in the past, the concept of so-called 'composed TOEs' and their security evaluation according to CC – refer to the specific assurance class ACO and the CAP packages for composed TOEs in [CC-1], [CC-3], [CC-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, as before 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

4 The overall composite evaluation approach is described in [CC-1], sections 14.2.1 and 14.3.3. Additional aspects are outlined in [CC-1], sections 14.4 and 14.5. Corresponding security assurance requirements (SARs) for specific composite evaluation aspects are specified in [CC-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.

5 The objective of this document is to address *composite certification* aspects that are relevant for scheme harmonisation and mutual recognition, but are not or only partly covered by the [CC] and especially the aforementioned [CC-1], [CC-3] and [CEM] sections. Hence, the purpose of the present document is to provide additional information, requirements and rules for *composite certification* procedures.

6 The composite evaluation approach as described in [CC-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 "Smartcards and Similar Devices"[1]. 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 regards the general composite evaluation approach addressed in [CC] and [CEM]. Where applicable, specific aspects for smart cards and similar devices are considered.

7 In the framework of composite evaluation and certification of composite products according to [CC] and [CEM], the present document replaces the JIL document "Composite product evaluation for Smart Cards and similar devices" ([JIL COMP 1.5.1]).

8 Specific examples and descriptions in [CC-1], section 14.3.3 illustrate the application of the composite evaluation approach in the area of smart cards and similar devices.

[1] The smart cards and similar devices technical domain is defined as: related to smart cards and similar devices where significant portions of the required security functionality depend upon hardware features at a chip level (for example smart card hardware/ICs, smart card composite products, TPMs (Trusted Platform Modules) used in trusted computing, digital tachograph cards, etc.) (source of definition: http//:www.sogis.eu).

2 Definitions and terminology

9 Definitions and terminology used in the framework of the composite evaluation approach are provided in [CC-1], sections 3 and 14.3.3.

10 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.

11 Due to specific requirements or constraints respectively concerning terminology used in ISO/IEC 15408:2022 series and ISO/IEC 18045:2022 and as consequence to being found in the derived [CC] and [CEM] (refer to ISO/IEC 15408-1:2022, section 3 and [CC-1], section 3) the following mapping of terms will be used in the present document:

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

Table 1 – Mapping of terms

3 Composite evaluation concept and approach

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

13 The role model for the composite evaluation approach is presented in [CC-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-1], sections 14.3.3.5, 14.3.3.6 and 14.3.3.7. In particular, Table 2 and Table 3 in [CC-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 respectively. Hereby, beyond the aforementioned requirements the required information shall be shared on a need-to-know basis according to the following table:

14

	Actors				
Documents/contributions to be provided to	**Composite product evaluation sponsor**	**Composite product integrator**	**Dependent component developer**	**Composite product evaluator**	**Composite product evaluation authority**
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 samples[2]	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

Table 2 – Specific deliveries between actors

[2] Only relevant for composite evaluation in the area of smart cards and similar devices: if requested by the composite product evaluator as defined in [JIL AP]

15 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.

4 ETR for composite evaluation

16 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-1], sections 14.3.3.5, 14.3.3.6 and 14.3.3.7.

17 Concerning the so-called ETR for composite evaluation (ETR_COMP) please refer to [CC-1], section 14.3.3.6 and 14.3.3.7. Here, 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 are provided. 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 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 is given in Appendix 1 of this document.

5 Composite evaluation rules and activities

18 Security assurance requirements (SARs) for specific composite evaluation aspects are specified in [CC-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-1], sections 14.2.1, 14.3.3, 14.4 and 14.5.

19 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-5], section 6.

20 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.

21 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.

22 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-1], section 14.3.3.5.

23 The current composite evaluation approach can be applied independent 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.

24 For applying the composite evaluation technique, it is assumed for the present document that the level of assurance of the base component is equivalent or higher compared to the composite product evaluation level. Other cases have to be discussed within the schemes.

6 Validity of reports, certificates and ETR for composite evaluation

25 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-1], section 14.3.3.7, but have to be supplemented accordingly for *composite certification* needs.

26 On base of [CC-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 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:

27 The rules and requirements on validity aspects including topicality and relevance as depicted in [CC-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 and that accompany the respective report.

28 The topicality for the ETR for composite evaluation in the technical domain of smart cards and similar devices is determined by the "Application of Attack Potential to Smartcards and Similar Devices" document ([JIL AP]) and the "Attack Methods for Smartcards and Similar Devices" document ([JIL AM]).

29 The ETR for composite evaluation has a validity limit of at maximum 18 months regards 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. 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.

30 In continuation of [CC-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 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 documents [JIL AP] and [JIL AM].

7 Rules, requirements and hints for composite certification

31 The following rules and requirements for *composite certification* of a composite product have to be applied:

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

33 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 schemes.

34 The current composite evaluation approach can be applied independent 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.

35 Composite evaluation and certification activities including evidence elements shall follow the rules depicted in sections 5, 6 and 6 of 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.

36 The composite product assurance package “COMP” in [CC-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-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.

37 For the composite product and its composite evaluation and certification, the composite product assurance package “COMP” in [CC-5], section 6 shall be claimed in the composite product Security Target.

38 Specifically, for the Technical Domain “Smartcards and Similar Devices” the latest available version of the JHAS documents for vulnerability analysis and penetration testing has to be taken into account.

39 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.

40 All composite evaluation-specific evaluator actions have to be documented according to the scheme rules and finalised by one of the verdicts PASS, FAIL or INCONCLUSIVE. As these actions are “refinements” of the traditional actions focused on the composite evaluation activities, these verdicts have to be integrated to the overall verdict.

41 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 case of chains of composite evaluations the entire list of re-used ETRs for composite evaluation has to be provided.

42 Assurance Continuity of composite certificates shall follow the general rules defined in [CC AC] 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, but specifically in the case of a change of the related base component this assessment is performed on base of the assessment of the changed base component by the base component evaluation authority.

8 References

8.1 CC:2022 and CEM:2022 documents

[CC] CC:2022 Release 1, covering

[CC-1] CCMB-2022-11-001: Common Criteria for Information Technology Security Evaluation, CC:2022, Part 1: Introduction and general model, Revision 1, November 2022

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

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

[CC-4] CCMB-2022-11-004: Common Criteria for Information Technology Security Evaluation, CC:2022, Part 4: Framework for the specification of evaluation methods and activities, Revision 1, November 2022

[CC-5] CCMB-2022-11-005: Common Criteria for Information Technology Security Evaluation, CC:2022, Part 5: Pre-defined packages of security requirements, Revision 1, November 2022

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

8.2 Supporting documents

[JIL COMP 1.5.1] Joint Interpretation Library – Composite product evaluation for Smart Cards and similar devices, Version 1.5.1, May 2018

[JIL AP] Joint Interpretation Library – Application of Attack Potential to Smartcards and Similar Devices, latest approved version

[JIL AM] Joint Interpretation Library – Attack Methods for Smartcards and Similar Devices, latest approved version (confidential document)

[CC AC] Assurance continuity: CCRA requirements, latest approved version

Joint Interpretation Library – Assurance Continuity, latest approved version

8.3 Templates

[ETR_COMP_SC+SD] Template – ETR for composite evaluation – TD SC & SD, latest approved version

Appendix 1: Template for ETR for composite evaluation

For the Technical Domain "Smartcards and Similar Devices" a specific ETR for composite evaluation-document (cf. [ETR_COMP_SC+SD]) is available. It bases on the general requirements regards the contents of an ETR for composite evaluation as outlined in [CC-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 ETR for composite evaluation-document shall be used as a template by the base component evaluator to issue the ETR for composite evaluation (ETR_COMP). Please note that the document layout may be customized according to the evaluation body's company standard, but the contents and structure are mandatory.

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

Terms used in [CC], [CEM] and the present document	**Terms used in [ETR_COMP_SC+SD]**
base component	platform
dependent component	application

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

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.

Appendix 2: Base component user guidance examples

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 for 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.

Appendix 3: Mapping [JIL COMP 1.5.1] – [CC] (informative)

The following table provides information about to which document sections of CC/CEM:2022 ([CC]) the contents of the former JIL Supporting Document "Composite product evaluation for Smart Cards and similar devices", ([JIL COMP 1.5.1]) were transferred to. Please note that [CC] mainly covers *composite evaluation* related topics, whereas *composite certification* aspects are supplemented by the present document (refer to section 1.2).

JIL Composite product evaluation for Smart Cards and similar devices, [JIL COMP 1.5.1]	**CC/CEM:2022 [CC]**
Section 2.1	[CC-1], section 14.3.3.1, 14.3.3.2, 14.3.3.3
Section 2.2	[CC-1], section 14.2.1, 14.3.3.4
Section 3.1	[CC-1], section 14.3.3.5
Section 3.2	[CC-1], section 14.3.3.5
Section 3.3	Refer to present document, section 7.
Section 3.4	[CC-1], section 14.3.3.5
Section 4.1	[CC-1], section 14.3.3.5
Section 4.2	[CC-1], section 14.3.3.5
Section 4.3	[CC-1], section 14.3.3.5
Section 4.4	[CC-1], section 14.3.3.5
Section 4.5	[CC-1], section 14.3.3.5
Section 4.6	[CC-1], section 14.3.3.5
Section 4.7	[CC-1], section 14.3.3.5
Section 5.1	[CC-1], section 14.3.3.6.1, 14.3.3.6.2
Section 5.2	[CC-1], section 14.3.3.6.1, 14.3.3.6.2 Refer to present document, section 4.
Section 5.3	[CC-1], section 14.3.3.6.3
Section 5.4	[CC-1], section 14.3.3.6.4
Section 6	[CC-1], section 14.3.3.7 Refer to present document, section 6 and 7.
Appendix 1	[CC-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-1], section 14.4
Appendix 2	Refer to present document, Appendix 1.
Appendix 3	Refer to present document, Appendix 2.

Table 4 – Mapping [JIL COMP 1.5.1] – [CC]