Open Smart Card Infrastructure for Europe

v2

Volume 8: **Security and Protection Profiles**

Part 3-2: **ETR-lite for composition: Annex A Composite smart card evaluation: Recommended best practice (Common Criteria Supporting Document)**

Authors: **eESC TB3 Protection Profiles, Security Certification**

NOTICE

This eESC Common Specification document supersedes all previous versions.

Neither eEurope Smart Cards nor any of its participants accept any responsibility whatsoever for damages or liability, direct or consequential, which may result from use of this document.

Latest version of OSCIE and any additions are available via www.eeurope-smartcards.org and www.eurosmart.com. For more information contact info@eeurope-smartcards.org.

Warning

This document is a Common Criteria supporting document. It is not officially endorsed by all the Common Criteria Recognition Arrangement participants, but is endorsed by some certificate-producing participants that use it in a particular field of technology. The use of this supporting document is not mandatory. It can be used by any certification/validation body, evaluation facility and vendors.

Any comments about this document can be sent to the sponsor of the document.

See the CCRA Procedure for Supporting Documents

Document name : ETR-lite for composition: Annex A Composite smartcard evaluation
: Recommended best practice

Reference : Version 1.2, March 2002

Object : Smartcards

Sponsor : DCSSI

Supporters : BSI, CESG, DCSSI, NLNCSA

Last update : March 2002

By : DCSSI

Table of Contents

1. General purpose

1 This document constitutes one of the annexes of the document *ETR-lite for composition* and is concerned with smartcard technology.

2 The objective of this document is to define the deliverables as output of an integrated circuit evaluation in order to perform a composite smart card evaluation. These deliverables can be part of the *ETR-lite for composition* document.

3 In this annex, a composite smartcard is considered as an integrated circuit with its embedded software. The embedded software is defined as the software embedded on the integrated circuit such as an operating system, general routines and interpreters (smartcard basic software) or a software dedicated to an application.

2. Field of special use

4 Smartcard evaluations.

3. Evaluation of a composite smartcard product

3.1 Introduction

5 The evaluation of a composite smartcard product requires the evaluation of the integrated circuit and the evaluation of its embedded software. During the embedded software evaluation, additional evaluation activities called "composition activities" have to be done. The composition activities are required to verify that weaknesses are not introduced by the integration of the composite product.

6 All evaluation activities required to certify a composite smartcard product are stated in the following table :

Assurance Requirements	**Integrated Circuit Evaluation Activities**	**Composite Smartcard Evaluation Activities**	
		Embedded Software Dedicated Activities	**Composition Activities**
ASE: Security Target	[CEM] & [CC-IC App]	Evaluation of the composite product Security Target	
ACM: Configuration management	[CEM] & [CC-IC App]	[CEM]	Integration of the embedded software in the IC manufacturer configuration management system

Assurance Requirements	**Integrated Circuit Evaluation Activities**	**Composite Smartcard Evaluation Activities**	
		Embedded Software Dedicated Activities	**Composition Activities**
ADO: Delivery and operation	[CEM] & [CC-IC App]	[CEM]	Consistency check for delivery and prepersonalisation procedures
ADV: Development	[CEM] & [CC-IC App]	[CEM]	Compliance with the IC user guidance
AGD: Guidancedocuments	[CEM] & [CC-IC App]	[CEM]	
ALC: Life cycle support	[CEM] & [CC-IC App]	[CEM]	
ATE: Tests	[CEM] & [CC-IC App]	[CEM]	Composite product functional testing
AVA: Vulnerability assessment	[CEM] & [CC-IC App]	[CEM]	Composite product vulnerability analysis

7 Therefore the evaluators of subsequent composite product evaluations will need to have access to detailed results of the integrated circuit evaluation in order to validate the effectiveness of the security requirements which are implemented by a combination of hardware and software. These detailed results have to be included in the *ETR-lite for composition* document.

8 The evaluator in charge of the composition activities needs sufficient skills in integrated circuit and embedded software evaluation. He has to rely on the information/deliverables from the integrated circuit evaluation in order to re-use the results. Therefore if different parties perform the evaluation, the composite product evaluator is not liable for the integrated circuit evaluation.

3.2 Composition activities

Evaluation of the composite product Security Target

9 A Security Target for the composite product has to be written and evaluated. The evaluator has to examine for any conflicting assumptions, conflicting non-IT requirements, compatibility of objectives and requirements and functionality needed by the embedded software but not part of the integrated circuit evaluation.

10 If the match between the integrated circuit security target and the composite product security target has been done at the level of the protection profiles they claim, the check is no more required.

11 The sponsor of the composite product evaluation must ensure that the following are made available to the evaluator :

- the security target or its public version (see concept of ST-lite) of the integrated circuit.

Integration of the embedded software in the integrated circuit manufacturer configuration management system

12 The evaluator of the composite product shall verify that the evaluated configuration management system of the integrated circuit manufacturer is actually used for the embedded software.

13 The sponsor of the composite product evaluation must ensure that the following are made available to the evaluator :

- the element of evidence for the use of the evaluated configuration management system of the integrated circuit manufacturer for the software to be embedded (e.g. configuration list).

Consistency check for delivery and prepersonalisation procedures

14 The composite product evaluator shall verify that delivery procedures of the embedded software are consistent with the acceptance procedures used by the integrated circuit manufacturer.

15 The composite product evaluator shall verify that prepersonalisation parameters defined by the embedded software developer are used by the integrated circuit manufacturer.

16 The sponsor of the composite product evaluation must ensure that the following are made available to the evaluator :

- the element of evidence for the embedded software reception and acceptance by the integrated circuit manufacturer,

- the element of evidence for the parameter acceptance and use.

Compliance with the integrated circuit user guidance

17 The composite product evaluator shall verify that recommendations for software developer (integrated circuit user guidance) have been taken into account in the embedded software development.

18 The sponsor of the composite product evaluation must ensure that the following are made available to the evaluator :

- the integrated circuit user guidance.

Product functional testing

19 The functional testing of the composite product shall be performed on samples.

20 The sponsor of the composite product evaluation must ensure that the following are made available to the evaluator :

- samples with the embedded software to be evaluated.

Composite product vulnerability analysis

21 The composite product evaluator shall perform a vulnerability analysis for the composite product using the results of the integrated circuit evaluation. This vulnerability analysis shall be confirmed by penetration testing.

22 During the composite product vulnerability analysis, the composite product evaluator has to investigate if the deactivation of an hardware security mechanism can be used to perform an attack on the composite product. If the analysis shows that an attack could be practicable, the composite product evaluator has to perform penetration tests on prepared samples.

23 Prepared samples are integrated circuits with the embedded software to be evaluated where an hardware security mechanism is deactivated by chip modification tools. These samples are used to perform the attack identified during the composite product vulnerability analysis.

24 The sponsor of the composite product evaluation must ensure that the following, as part of the *ETR-lite for Composition* document, are made available to the composite product evaluator :

- the list of the integrated circuit security mechanisms. For each mechanism, the generic type of the attack which have been performed during the integrated circuit evaluation and the effort needed to achieve the attack shall be provided (see [AP-SC] for the calculation of the effort).

- if required, information for deactivating the integrated circuit mechanisms or already prepared samples.

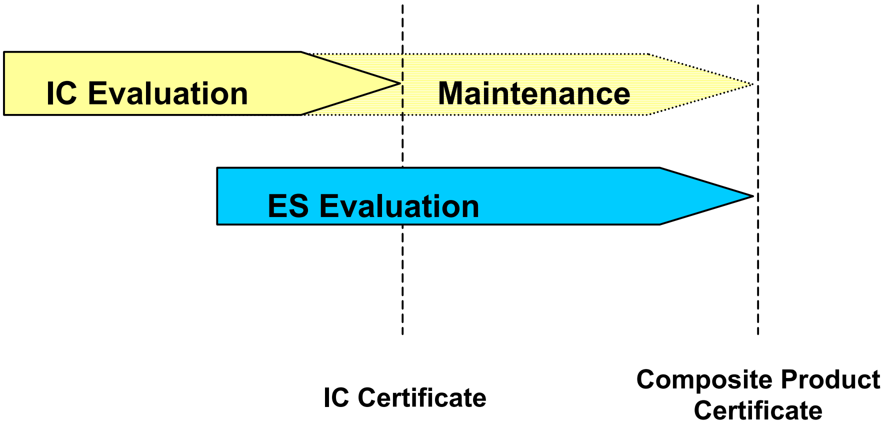
4. Use of a certified integrated circuit

4.1 Objective

25 The objective is to use efficiently the results of the evaluation of an integrated circuit for the evaluation of a composite smartcard product.

4.2 Case 1: Maintenance

26 The results of the evaluation of the integrated circuit can be integrally re-used if the integrated circuit is certified and covered by a maintenance programme. This maintenance programme has to be consistent with the CC approach with, in addition for smartcard, independent penetration testing as part of each maintenance step, where necessary.



4.3 Case 2: No maintenance

27 If the certified integrated circuit is not covered by a maintenance programme, the results of the following evaluation tasks have to be reviewed by the certification bodies and where necessary updated :

- strength of functions and vulnerability analysis to verify that :
    - new vulnerabilities or new attacks have not been discovered,
    - vulnerabilities found in the previous evaluation did not become exploitable now due to the increase of performance of tools available,
- integrated circuit development and production environment evaluation to verify that the configuration management system, the organisational security measures and the delivery procedures are still applied.

Case 2a: Re-certification

28 By the re-certification process, the certification body certifies that the previous integrated circuit evaluation results remain valid or that results have been updated by the integrated circuit evaluator.

29 With an integrated circuit re-certification, the results of the integrated circuit evaluation can be integrally re-used for the composite product evaluation.

Case 2b: Updating as part of the composite product evaluation

30 In case the integrated circuit is neither covered by a maintenance programme nor re-certified, the composite product evaluator has to verify that the previous integrated circuit evaluation results remain valid or, if necessary, he has to update the results.

31 The sponsor of the composite product evaluation must ensure that the following are made available to the composite product evaluator :

- ACM, ALC_DVS and ADO_DEL deliveries,

- AVA_SOF and AVA_VLA deliveries.

32 If available by the integrated circuit manufacturer, the associated evaluation reports or a part of the reports can be provided to the composite product evaluator in order to limit the activities to be performed.

5 References

33 These references are correct in march 2002 but may be updated subsequently.

[CC] Common Criteria for Information Technology Security Evaluation, Version 2.1, August 1999.

[CEM] Common Methodology for Information Security Evaluation (CEM), Part 2, Version 1.0, August 1999.

[CC-IC App] The Application of CC to Integrated Circuits, version 1.0, January 2000.

[AP-SC] Application of Attack Potential to Smartcards, version 1.0, March 2002.