

Open Smart Card Infrastructure for Europe

V2



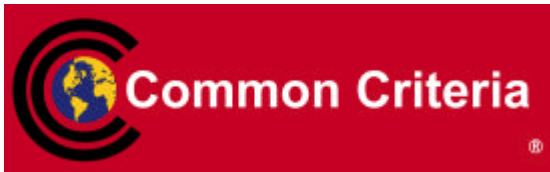
Volume 8: Security and Protection Profiles

**Part 3-1: ETR-lite for composition (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 use 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
Reference : Version 1.1, July 2002
Object : Composition of certified components
Sponsor : BSI
Supporters : BSI, CESG, DCSSI, NLNCSA

Last update : July 2002 (draft indicator deleted, same content as V1.0)

By : BSI, CESG, DCSSI, NLNCSA

1.General purpose:

In cases where evaluators responsible for performing an evaluation of a composite product which uses a certified/validated product, need to get specific information from the previous evaluation and the ETR cannot be supplied, the information has to be supplied in an additional document. This document has to be shared beyond the original audience (developer, ITSEF, CB of the certified TOE). In due course an annex will be provided for each technology.

2.Field of special use: Evaluation of Smartcard Components

3. Body text:

Table of contents

1	Introduction.....	4
2	Objectives	5
3	Requirements for specification of the content of the <i>ETR-lite for composition</i>	5
3.1	Generic rules:	5
3.2	Content of the ETR-lite for composition	6
3.2.1	TOE design.....	6
3.2.2	Evaluated configuration.....	6
3.2.3	Delivery procedures and data exchange.....	7
3.2.4	Testing	7
3.2.5	Observations and recommendations	7
4	List of Annexes	8

1 Introduction

1 The CC aims to provide Users with increased assurance that a product fulfills their security needs (CC Part 1, section 3.2.1). It discusses the CC in the context of Developer, Evaluator and User and notes the potential involvement of other groups, including the evaluation Sponsor and Evaluation Authority (Certification Body).

2 In some cases there are specific subsequent "users" of the TOE such as evaluators from the ITSEF performing an evaluation of a composite product using the TOE. These specific "users" are not the end user of the TOE, but that nevertheless need to obtain specific information from the TOE evaluation.

3 Other subsequent "users" might be those users of the certified product not involved in the evaluation process (e.g. card issuers or type approvers required for risk analysis). The interests of these users is not addressed by this document.

4 Security requirements are defined in a Protection Profile or Security Target. As these are typically public documents, they avoid or at least sanitise, vulnerability and attack potential detail. Common Evaluation Methodology and the CC Certificate also avoid such detail owing to their public nature.

5 The standard Evaluation Technical Report (ETR) as defined by the schemes contains proprietary information that cannot be made public usually for both for security and commercial reasons. It contains:

- specific information of the evaluation performed (e.g. information about attacks which would assist an attacker in reducing the effort needed to mount a successful attack - knowledge which the CB and the vendor might wish to control),
- details of the design of the product which the vendor wishes to keep confidential as well as
- proprietary evaluation techniques or tools.

6 While the original sponsor may have access to detailed information in the ETR, the evaluators from the ITSEF performing an evaluation of a composite product using the TOE would not have access in general. In principle, the ETR could be supplied to specific "users" under a nondisclosure agreement if all parties would agree, but practice shows that this is not possible for confidentiality or commercial reasons in most cases.

7 On the other hand, the information in the certification report (CR) specified within Annex I of the CC Mutual Recognition Arrangement (CC-MRA) is not detailed enough for the purposes and interests of these specific users. It leaves them with high-level statements of threats and defenses, but not enough information to know exactly how the product was tested, which vulnerability analyses were performed or penetration scripts covered. This is especially problematic in the areas where technology is evolving very rapidly (e.g. in the smartcard field).

8 Therefore, in those cases where evaluators from the ITSEF responsible for performing an evaluation of a composite product which uses the TOE, need to

get specific information from the TOE evaluation and the ETR cannot be supplied, the information has to be supplied in an additional document. This document has to be shared beyond the original audience (developer, ITSEF, CB of the certified TOE). In due course an annex will be provided for each technology.

2 Objectives

9 For evaluators from the ITSEF performing an evaluation of a composite product using the TOE, the issue mentioned above can be resolved by compiling specific information from the ETR into a document named *ETR-lite for composition*.

10 The information contained in the *ETR-lite for composition* enables the specific “user“ to understand threats and the effectiveness of countermeasures. It provides additional information about the evaluation results compared with publicly available information (e.g. Certification Report). It should be a subset of the ETR and must be usable for the specific needs of evaluation composition. Even though it is a controlled document it must be available to specific users.

11 *ETR-lite for composition* is not intended to be used for a re-evaluation of a certified TOE. In this case the ETR is necessary.

12 The *ETR-lite for composition* is not intended to be used for those “users“ of the certified product not involved in the evaluation process (e.g. for risk analysis purposes for issuers or type approvers). Issues concerning these “users“ are not covered by this document. An additional document might be required.

3 Requirements for specification of the content of the *ETR-lite for composition*

3.1 Generic rules:

13 The *ETR-lite for composition* should be produced by the ITSEF responsible for evaluating the TOE based on the content of the ETR. This task should be considered when determining the evaluation work programme to reduce additional cost and effort.

14 The detail contained in *ETR-lite for composition* has to strike the right balance between keeping developer and/or laboratory proprietary information secret and providing sufficient information for the specific user.

15 *ETR-lite for composition* shall not include information which affects national security.

16 The information provided must be approved by all parties involved in the evaluation (i.e. the ITSEF, the certification body and the developer and sponsor of the evaluation). The certification body or the ITSEF shall check consistency with the original ETR. The certification report will reference *ETR-lite for composition*, if available.

17 *ETR-lite for composition* will be a document marked *commercial in confidence* and shall be available only to specific "users" under conditions determined by the parties involved (e.g. a binding nondisclosure agreement). Access to *ETR-lite for composition* shall be controlled by the developer who is in charge of the document control for the TOE.

18 It is assumed, that the security target and the guidance documentation for the TOE are available to the audience of the *ETR-lite for composition*. The TOE should also be made available for composition evaluation.

3.2 Content of the ETR-lite for composition

19 The information required is focused on:

- a) Specific formal information e.g. reference to the certification report and the ETR
- b) Specific information about the TOE design
- c) Information about the evaluated configuration of the TOE
- d) Information on delivery procedures
- e) Information about functional and penetration testing of the TOE
- f) Observations and recommendations

3.2.1 TOE design

20 This section provides a high-level description of the IT product and its major components based on the deliverables described in the Common Criteria assurance family entitled Development-High Level Design (ADV_HLD). The intent of the section is to characterise the degree of architectural separation of the major components and to show dependencies between the TOE and products using the TOE in a composition (e.g. dependencies between HW and SW).

21 For vulnerability assessment of a composite TOE, information on security mechanisms and possibilities for deactivation can be necessary to perform the vulnerability analysis of the composite TOE. Therefore, specific evaluation evidence of the ADV class (mostly about ADV_FSP) may be necessary.

3.2.2 Evaluated configuration

22 This section provides specific information about the evaluated configuration of the TOE as per part of ACM_SCP based on the developers' configuration list or relevant parts as needed or on a case by case basis.

23 If applicable for the TOE, security relevant generation or installation parameter settings should be explained and their effect on the defense of attacks be outlined. For TOE generation, this might be beyond the information about TOE installation provided in the guidance documents but it is part of ADO_IGS in the ETR.

24 Specific Evidence about the evaluation of the configuration management coverage (ACM_CAP) can be necessary for a specific type of TOE if it is relevant for supporting composite evaluations (e.g. evidence about integration of a SW-TOE in the configuration management of a combined HW/SW-production). Therefore, beside the evaluation evidence about the principle

capability of the configuration management system, a specific configuration list containing the composed TOEs may be necessary.

3.2.3 Delivery procedures and data exchange

25 For supporting composition evaluation of specific TOEs, evaluation evidence can be necessary for delivery, reception and acceptance procedures of TOEs and related data to be composed and exchanged during development and production. Therefore, evaluation evidence about ADO_DEL and ALC_DVS can be relevant.

3.2.4 Testing

26 This section provides specific information about the testing of the security functions of the TOE and penetration tests. This includes both, the developer and evaluator testing effort, outlining the testing approach, configuration and depth. This includes information about tools used for testing.

27 Test coverage information shall outline what functionality, technical or security features, including their interfaces, have been tested.

28 Information about penetration testing shall give a list of the types of penetration attacks analysed for the TOE. It should include details necessary for understanding the effort done for a penetration test and should help to understand the value of the test results in the context of improved test equipment and methods over time.

29 In accordance with the requirements of CEM (see for example CEM part 2 version 1: 4:ATE_FUN1-12, 4:ATE_IND.2-11, 4:AVA_VLA.2-8), this information is available within the ETR. So it can be compiled for *ETR-lite for composition*.

30 If a "user" requires specific tests of the TOE, this should be considered in the evaluation approach and covered during developer and evaluator testing for ATE and AVA. These tests should be specifically mentioned in *ETR-lite for composition*.

3.2.5 Observations and recommendations

31 The evaluated guidance documentation shall contain all information required to use the TOE in a secure way as defined in the security target including recommendations on how to avoid residual vulnerabilities and the unexpected behaviour that has been described.

32 However, in specific cases detailed information might be required in addition to the guidance documents such as:

- information on observations resulting from the evaluation (e.g. unexpected behaviour outside the operational envelope).
- vulnerability information, comprising: vulnerabilities defeated by the TOE, residual vulnerabilities counteracted by environmental measures, residual vulnerabilities, possibly exploitable with higher attack potential (see e.g. CEM 4:AVA_VLA.2-16).

- specific information for evaluators making use of the evaluation results (e.g. about specific testing necessary during a composition evaluation).

4 List of Annexes

33 The annexes are provided as separate documents.

34 Annex A:

Composite smartcard evaluation : Recommended best practice, IC and ES composition, Version 1.2