brightsight®

your partner in security approval

Enhancing the Well-Defined and Successful ETR for Composition Approach

Monique Bakker, Olaf Tettero
11 September 2013; commoncriteria@brightsight.com

Goal of this presentation

1. What should be the content of the ETR for Composition

2. The role of the ETR for composition during the composite evaluation

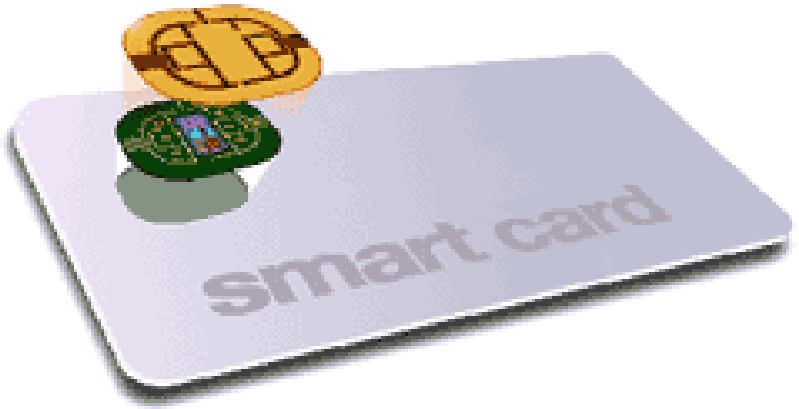
ETR for Composition

- Used in the smartcard domain
- Used to facilitate composite evaluations for embedded smartcard software
  - CardOS on (crypto library) and hardware platform
  - Cryptographic library on hardware platform
  - Applet on Card/OS/Hardware platform
- Allows reuse of results of underlying platform certification

JIL document: Composite product evaluation for Smart Cards and similar devices, version 1.2, January 2012

CCDB-2007-09-002: ETR template for composite evaluation of Smart Cards and similar devices

CCDB-2012-04-001: Composite product evaluations for smart card and similar devices

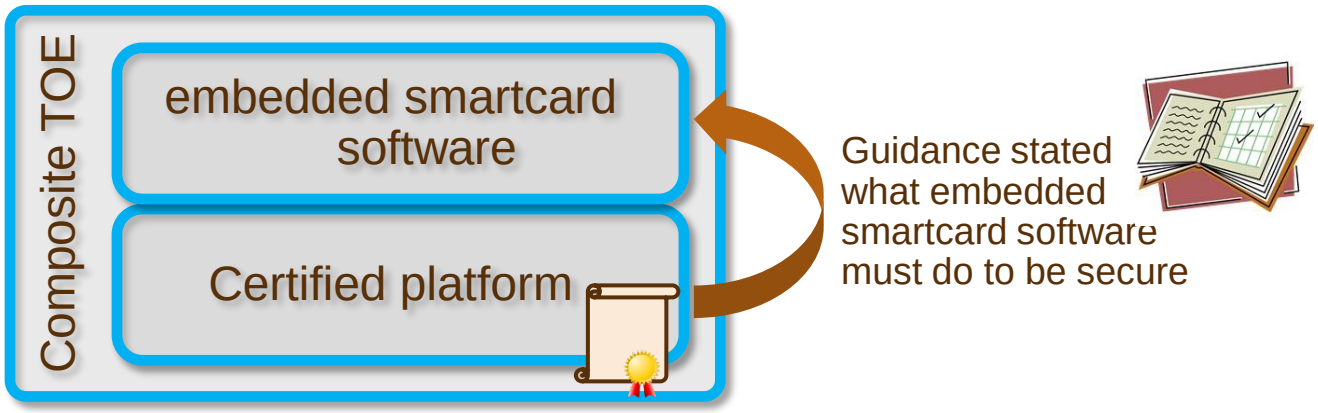


What does ‘ETR for composition’ arrange?

- Understanding of the effectiveness of countermeasures of the platform
- Supports assessment of the composite TOE evaluator:

  “*Is the composite TOE resistant against attackers with a high attack potential*?”

Note:
This document is not available to the embedded smartcard software developer



ETR for Composition – Main contents

- Platform description including *security mechanisms*
- Evaluated configuration
- Delivery procedure for platform
- Penetration tests performed by platform evaluation laboratory
  - Test configuration
  - Description
  - Attack rating
- Summary of vulnerability analysis
- Recommendations regarding the guidance

Composite evaluation perspective

Goal ‘ETR for Composition’ approach

- Overall evaluation becomes more efficient
- Means for proper vulnerability analysis on the TOE as a whole

ETR for Composition supports the composite evaluation lab to assess whether the embedded smartcard software fulfils all requirements from ETR for composition

Practice

1. Not conclusive on protection against a certain attack
2. Composite evaluation lab must do additional tests (possibly redundant)
3. Additional design information is needed, whereas this is preferably not available to the Composite evaluation lab
4. Should statements causes confusion

Bad news for efficiency

In case of a poor ETR for Composition…

- ETR is less than a year old; tests are performed more than two years ago
- Statements are ambiguous

"IC HW was found vulnerable"

"Guidance exists"

"Cryptographic library was not found vulnerable"

"Severe attack not considered for Cryptographic algorithm A"

"Recommendation is confirmed"

So … What to do as composite evaluator?

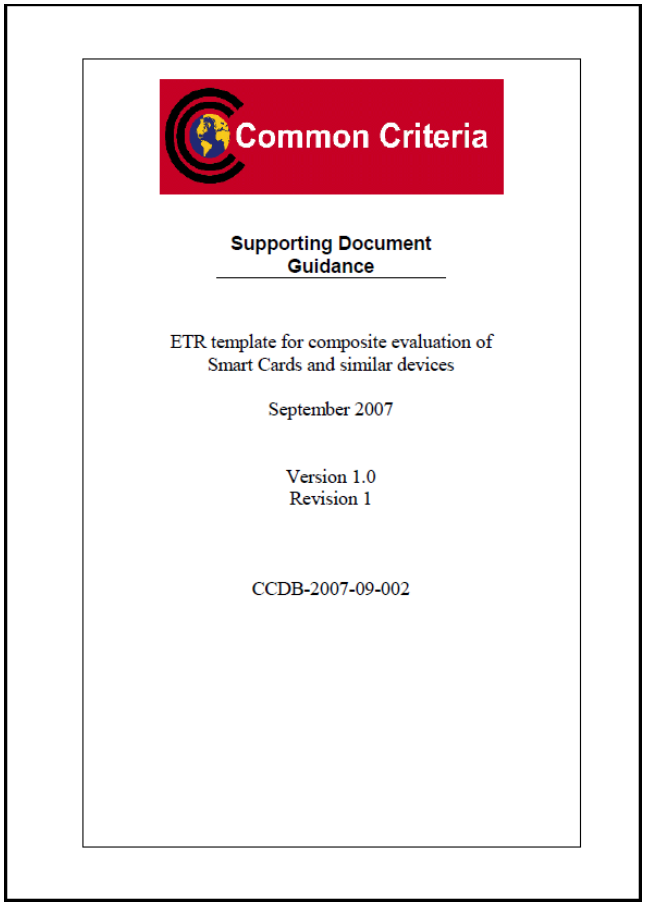
- Re-do a test to understand the result
- Do a lot of tests to get the assurance
- Reverse engineer the platform
- Stop the evaluation,
  not enough information to complete

How to recognize a good ETR for composition?

Suggestions to refine CCDB-2007-09-002

- Align contents of 'ETR' (CEM par. 112) and 'ETR for composition': *no additional review*
- Recognize that this document is not meant for the embedded smartcard software developer
- Recognize that ETR_COMP is of concern to two third-parties: composite evaluator and scheme
- Split the recommendations in ETR_COMP
  - for composite evaluator for testing
  - for guidance to embedded smartcard software Developer for emphasis on the mandatory recommendations

  Last one can be used in the Certification Report
- Make it mandatory in template


Common Criteria

Supporting Document
Guidance

ETR template for composite evaluation of
Smart Cards and similar devices

September 2007

Version 1.0
Revision 1

CCDB-2007-09-002

The centrale role of the ETR for composition

ASE_COMP: relevant platform TSF

ADV_COMP : design compliance

ATE_COMP : integration testing

AVA_COMP 1-1: reuse of vulnerability assessment on the platform

AVA_COMP1-2 : penetration test on product as a whole

ETR_COMP: which attack scenarios are tested and considered

ADV_ARC / GUID :
Relevant security services of underlying platform

Protection against attacks as specified in the JIL-Attack method

ADV_ARC –GUID : CCDB-2012-04-003 and CCDB-2012-04-004

brightsight®

The ETR for composition evaluation effort

ADV_COMP:

The developer implements recommendation

X, Y, Z

ETR_COMP: the TOE provides protection against attack (scenario) A, if the user adheres to embedded software recommendations X, Y, Z

ADV_ARC:

attack A covered during the hardware evaluation.

Attack A is analysed and not considered a potential vulnerability during AVA_VAN if conditions for reuse are met

The ETR for composition evaluation effort

ADV_COMP:

The developer does not implement recommendation

D, E, F

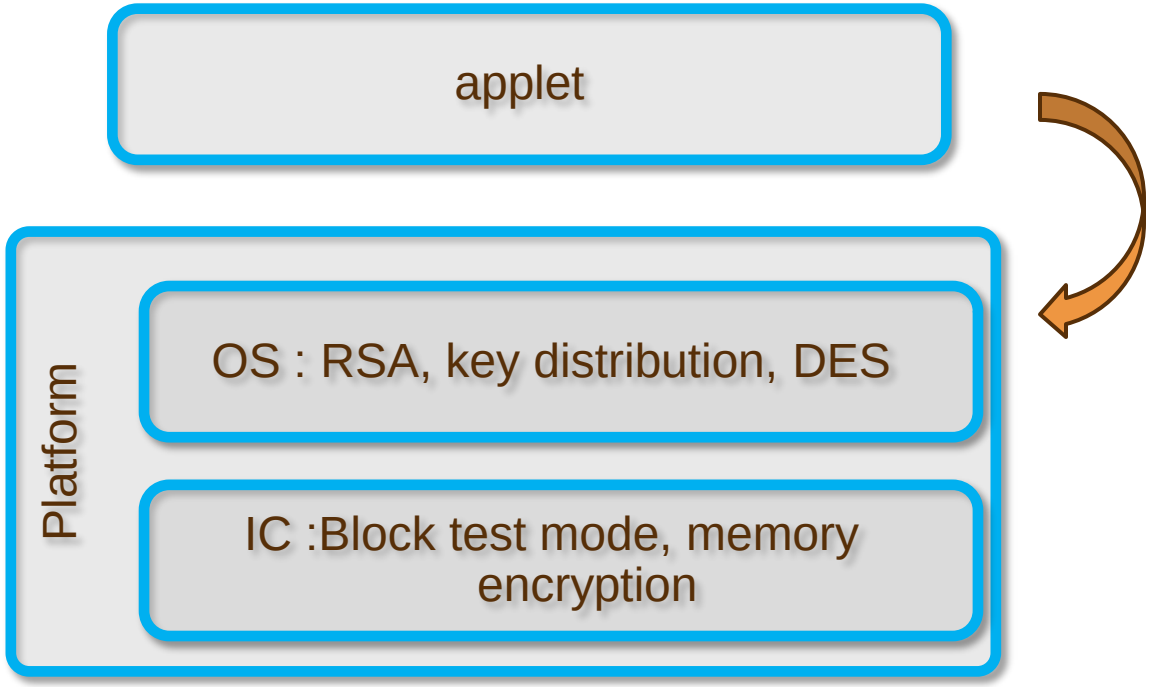
ETR_COMP: the TOE provides protection against attack (scenario) B, for service X if the user adheres to embedded software recommendations D,E,F

ADV_ARC:

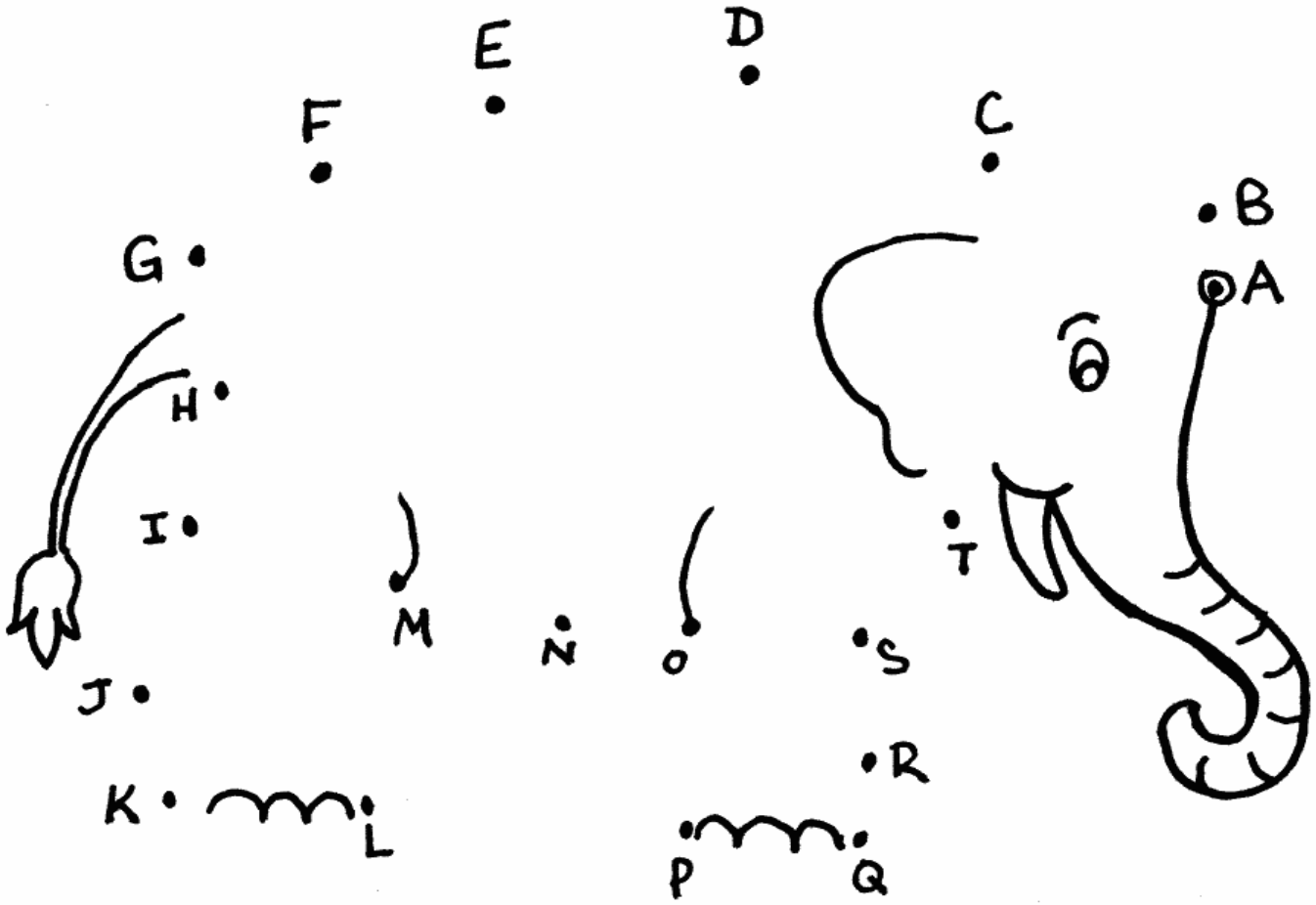
Security service X of underlying hardware platform is not listed

Attack B for service X is analysed and not considered a potential vulnerability during AVA_VAN

Is the applet developer able to identify all relevant services of the platform?



Create smaller substeps to achieve the same goal

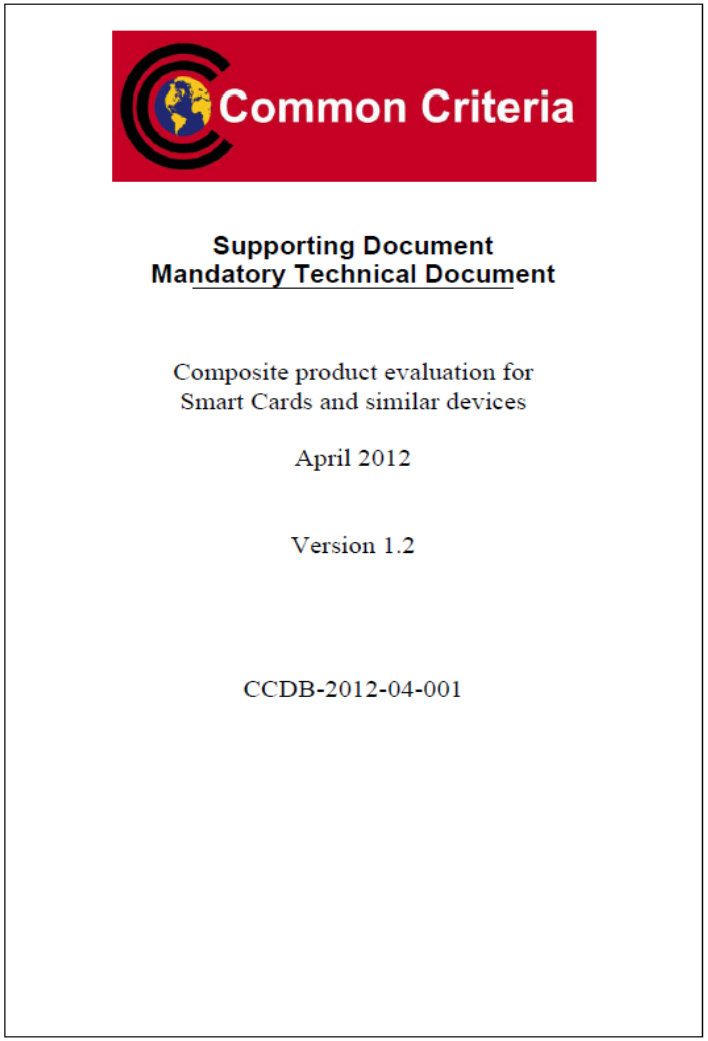


Suggestions to refine the methodology

Create methodology (in multiple steps) that actively evaluates the content of ADV_ARC /GUID in relation to the available information

Make sure the composite evaluator has a complete ETR for compostion from the template description

Separate methodology for the platform evaluator and the application evaluator?


Common Criteria

Supporting Document
Mandatory Technical Document

Composite product evaluation for
Smart Cards and similar devices

April 2012

Version 1.2

CCDB-2012-04-001

Questions?