



ISO/IEC JTC 1/SC 27
Information technology - Security techniques
Secretariat: DIN, Germany

DOC TYPE: Defect Report

TITLE: Defect Report to ISO/IEC 15408:2008 parts 2 and 3 and for ISO/IEC 18045:2008

SOURCE: WG 3 Experts and CCDB Liaison Statement (SC27N8023)

DATE: 2009-11-03

PROJECT: 15408-2, 15408-3, 18045

STATUS: This document was made available at the 39th SC 27/WG 3 meeting held in Redmond, US, 2nd – 6th May 2009. It is circulated within SC 27 for information.

ACTION ID: FYI

DUE DATE:

DISTRIBUTION: P-, O-, and L-Members
W. Fumy, SC27 Chairman
M. De Soete, SC27 Vice-Chair
E. J. Humphreys, K. Naemura, M. Ohlin, SC 27/WG Conveners
T. Chikazawa, SC 27/WG2 Secretariat

MEDIUM: Livelink-Server

NO. OF PAGES: 1+7

DEFECT REPORT

The submitter of a defect report shall complete the items in Part 2 and shall send the form to the Convener or the Secretariat of the WG with which the relevant editor's group is associated.

The WG Convener or Secretariat shall complete the items in Part 1 and circulate the defect report for review and response by the appropriate defect editing group.

The defect editor shall complete Part 4 and submit the completed report to the Convener or the Secretariat of the WG.

PART 1 - TO BE COMPLETED BY WG SECRETARIAT
DEFECT REPORT NUMBER: 15408-2/001, 15408-3/001, 18045/001
WG SECRETARIAT: WG3
DATE CIRCULATED BY WG SECRETARIAT: 2009-11-04
DEADLINE ON RESPONSE FROM EDITOR: 2009-12-15

PART 2 - TO BE COMPLETED BY SUBMITTER
SUBMITTER: CCDB Liaison Officer
FOR REVIEW BY: ISO/IEC JTC 1/SC 27/WG 3
DEFECT REPORT CONCERNING: 15408-2:2008 , 15408-3:2008 , 18045:2008
QUALIFIER: Error
REFERENCES IN DOCUMENT: See detailed list in appendix.
NATURE OF DEFECT The following defects were found by CCDB during their maintenance of the "Common Criteria" (CC), which are the documents corresponding to ISO/IEC 15408 and 18045. They were corrected in Revision 3 of the CC/CEM Version 3.1, as described in the CCDB Liaison Statement SC27N8023. Therefore CCDB and WG 3 experts propose to correct these defects also in ISO/IEC 15408 and 18045. All defects in essence impact two parts of the CC, the CEM, and corresponding ISO/IEC 15408 and 18045; however, since all requirements are derived from a single source document and are then propagated to other documents, one defect report is deemed sufficient.
SOLUTION PROPOSED BY THE SUBMITTER Correct defects as technical corrigenda preferably to be published as corrected reprints of the applicable documents.

PART 3 - EDITOR'S RESPONSE

Annex for Defect Report SC27N8120: Detailed list of defects for 15408-2:2008, 15408-3:2008, 18045:2008

This annex contains the detailed list of defects as identified by CCDB and WG 3 experts. The identifiers used by CCDB are included in order to enable the editor to identify the changes as made in the CCDB documents. Note that the exact text for the necessary changes is available in the "Common Criteria" documents, Version 3.1, revision 3 and can be identified using the XLS-Files contained in attachment 2 to the Liaison Report from CCDB (27N8023). The attachment has the file name "27N8023_Att_2_Rel3Changes.zip".

- KR-002: Editorial errors - Changes in FAU_SEL.1.1
Events were not audited, but will be audited (Cf. para 113).
- KR-003: Editorial Errors - Definition of LUB and GLB in Part 2 Para 187
Simple editing errors
- KR-004,008-01: TSF self test for each type of TSF(i.e., SW, HW, and/or FW)
FPT_TST.1 must include requirements for each type of TSF, i.e., TSF software, hardware, and/or firmware.
- KR-005-01: Editorial Errors - Reference error in Part 2 Para 868
Simple editing errors in annex F.8, FDP_ITT.4
- KR-007-01: Description Errors - FPT_TEE in Part 2, Annex J.12
Description errors in Part 2, J.12, FPT_TEE
- KR-011: Description Errors - EAL6 details in Part 3, subclause 8.8
Internally inconsistent description of TSF internals requirement of EAL6 against EAL7
- KR-012,013: Editorial Errors - ADV_FSP.2.5C, ADV_FSP.3.5C
Internally inconsistent description of ADV_FSP.2.5C against ADV_FSP.*.*C Security enforcing actions from ADV_FSP.3.5C should be defined as SFR-enforcing actions
- KR-014,021: Unclear requirements and work units - ADV_TDS.3.7C, ADV_TDS.4.7C
There are three "interaction" requirements in ADV_TDS.3 and ADV_TDS.4, i.e., 7C, 8C and 9C. From CC Part 3, it is unclear among these requirements, but from CEM, "interaction" from 7C can be considered as a "relationship". Thus it makes more clear requirement if using "relationship" for 7C. And work units for 7C should explicitly include examination on "relationship".
- KR-015: Editorial error and internal inconsistency - ADV_TDS.6.7C
Simple editorial error. And ADV_TDS.6.7C should include entire requirements of ADV_TDS.5.7C.
- KR-017: Unclear Developer action elements - ALC class
The developers must provide their evidence to evaluator.
- KR-018: Insufficient work units - APE_SPD.1-3, ASE_SPD.1-3
There is no work unit for examination or the OSPs.

- KR-019-01: Improper example - ADV_TDS.2
ADV_TDS.2 uses implementation representation as examples for other evidence, but ADV_IMP.1 requires ADV_TDS.3 as dependencies. Thus implementation representation is not available for ADV_TDS.2.
- KR-022: Editorial errors in work units for ADV_TDS.3, ADV_TDS.4
Simple editing errors - Misplacing paragraphs. Move paragraphs under ADV_TDS.3-9 and ADV_TDS.4-11 to somewhere under ADV_TDS.3-8 and ADV_TDS.4-10.
- KR-023,024: Improper guidance for ADV_TDS.3-11, ADV_TDS.3-12
Guidance paragraph under ADV_TDS.3-11 is not proper for the purpose of ADV_TDS.3-11. There exists duplicated guidance under ADV_TDS.3-12.
- KR-025: Insufficient work unit and improper guidance for ADV_TDS.3-13
There is no guidance for the verification of accuracy of the mapping in ADV_TDS.3-13. And some guidance under ADV_TDS.3-13 is not proper for the purpose of ADV_TDS.3-13.
- KR-027,028: Inconsistent use of terms - preparative procedures, duplicated guidance for AGD_PRE.1-2
Inconsistent use of terms - preparative procedures Duplicated guidance for AGD_PRE.1-2. One of them should be deleted.
- KR-029,030: Editorial error, insufficient work unit for ALC_CMC.4
Simple editorial error in ALC_CMC.4-2. Insufficient work unit - ALC_CMC.4-4 should address all configuration items identified under ALC_CMS.
- KR-031: Inadequate guidance for ALC_DVS.1-2
Security objectives for the development environment are not defined in the ST.
- KR-032-01: Inadequate guidance for ATE_DPT
Subsystem interfaces are not defined term. They should be expressed using "subsystem behaviour or interaction description". For ATE_DPT.2, depth of testing analysis for SFR-enforcing module should be examined.
- KR-020: Insufficient work unit for ADV_TDS.3 and ADV_TDS.4
Both ADV_TDS.3 and ADV_TDS.4 require a description of each subsystem of the TSF, i.e., SFR-enforcing, SFR-supporting and SFR-non-interfering. ADV_TDS.3-4 and ADV_TDS.4-6 are work units for examination of SFR-enforcing and SFR-supporting subsystems. There is no work unit for SFR-non-interfering. Renumber work units.
- CP-London-2008-GE-2007-0007
Part 2, changes in FDP_UCT and _UIT: The actions described in the SFRs should not only be possible, but be enforced.
- CP-London-2008-GE-2007-0014
CEM, ASE_TSS.1-1 and .2-1: It shall be possible to group SFRs for the description.
- CP-London-2008-GE-2007-0026
ADV_TDS.1.6C et al - Direction of Mapping between TSFI and TOE design was inconsistent.

- CP-London-2008-GE-2007-0034
Part 3, The word "focused" is missing in the text of AVA_VAN.3.3E.
- CP-London-2008-GE-2007-0047
Part 3, Appendix A 4.2: The example used in Appendix A.4.2, paragraph 591 requires a level of description that is not aligned with the criteria. This needs to be changed.
- CP-London-2008-GE-2007-0048
Part3, A.4.2: The definition what makes a module "SFR-enforcing" is not correct. A module must be declared as SFR-enforcing, even if it implements only a significant portion of an SFR.
- CP-London-2008-GE-2007-0049
CP London 2008 GE-2007-0049, Part 3 and CEM: eliminate requirements for algorithmical identical, since this is inconsistent with the requirements defined elsewhere
- CP-London-2008-GE-2007-0051
Part3, A.4.2: What needs to be described for a module depends on the level of ADV_TDS chosen and the characterization of the module as "SFR-enforcing", "SFR-supporting", or "SFR-non interfering". This is not correctly reflected in para 587.
- CP-London-2008-GE-2007-0052
Part3, ADV_TDS.3.8C: ADV_TDS.3.8C seems to require that a SFR-enforcing module needs to describe all interfaces to other modules it calls. This would imply also the description of interfaces to modules designated as "non SFR-enforcing". On the other hand there is no need that the description of those modules contain a specification of their interfaces. This is inconsistent and needs to be modified.
- CP-London-2008-GE-2007-0053
Part3, ADV_TDS.4.8C: The same inconsistency as for ADV_TDS.3.8C.
- CP-London-2008-GE-2007-0054
Part3, A.4.2 para 589: The document is inconsistent when global data has to be considered to be an interface. Para 589 states:

... "as well as implicit interfaces (e. g., global data manipulated by the module)."

This gives the impression that global data is regarded as an interface only when the module manipulates (i. e. changes) the global data. This view is supported by para 592, which states that only changes to global data need to be noted in the "algorithmic description" of a module.

On the other hand, para 589 also states in its last sentence:

"Global data should be described as to whether it is read or written (or both) by the module."

This inconsistency needs to be removed.
- CP-London-2008-GE-2007-0061
CEM, ATE_IND.2-2: Add full stop to clause, i.e. "... and is in a known state."
- CP-London-2008-GE-2007-0062

CEM, ATE_IND.2-3: Add full stop to clause, i.e. "... by the developer to functionally test the TSF."

- CP-London-2008-GE-2007-0063

CEM, ATE_IND.2-5: In this WU the evaluator shall check that the test results are consistent with the actual results. If disagreements cannot be resolved (c.f. par. 1370) the evaluator shall increase his sample size and the developer shall provide either corrective action on the tests or provide new tests.

However this "failed" tests could also indicate deficiencies in the TOE/TSF itself, hence a possible solution would be for the developer to correct the TOE/TSF as well. As written, it appears as if the developer should "test around" the failed test(s) instead of solving the issue behind it (which, of course, might be an incorrect test).

- CP-London-2008-GE-2007-0068

CEM, ADV_FSP.4-8 et al ADV_FSP.4-8 requires the evaluators to examine the functional specification for a complete and accurate description of all error messages resulting from an invocation of each TSFI.

ADV_FSP.4-9 requires the evaluators to examine the functional specification for a complete and accurate description of the meaning of all errors associated with each TSFI.

Considering that the description of all error messages associated with each TSFI was not verified before, the examining of the meaning description of all error messages associated with each TSFI can not be asked in this work unit, because only the subset "error messages resulting from an invocation" of all errors associated with each TSFI was examined before.

- CP-London-2008-GE-2007-0071

Part 3, CEM, "AVA_VAN.3 et al missing dependencies from ATE":

The work units AVA_VAN.3-6 (§ 1519) and AVA_VAN.4-6 (§ 1576) refer to the assurance family ATE_DPT in the context of developer testing evidence having to include testing performed to confirm the correct implementation of any specific mechanisms detailed in the security architecture description (ADV_ARC).

According to the paragraphs quoted above the evaluator shall use the results of ATE_DPT for developing the strategy for penetration testing in order to ensure that all aspects of the security architecture description are tested.

On the other hand, the assurance family ATE_DPT is not listed as a formal input for the respective evaluator actions.

- CP-London-2008-GE-2007-0072

Part 3, Dependencies of AVA_VAV.* on ADV_FSP.* are missing or inconsistent.

- CP-London-2008-GE-2007-0073

P3, inconsistent TSFI definitions:

CC 3.1R2, paragraph 222 as well as paragraph 542 characterize the TSFI as:

The TSFIs consist of all means for users to invoke a service from the TSF (by supplying data that is processed by the TSF) and the corresponding responses to those service invocations.

This characterization seems to imply that only interfaces a user can call and provide parameter are part of the TSFI. This leads to a conflict with requirement ADV_FSP.5.7C

which requires to "describe all error messages that do not result from an invocation of the TSFI". Those error messages are quite often returned at an "output only" interface (e. g. a log file or a message to an administrator). According to the characterization given in paragraphs 222 and 542 of part 3, those interfaces are not part of the TSFI and it remains unclear, how those error messages need to be described as part of the TSFI.

In addition the characterization of the TSFI in paragraphs 222 and 542 of part 3 is inconsistent with the definition of TSFI in part 1, which states:

TSF interface (TSFI) - a means by which external entities (or subjects in the TOE but outside of the TSF) supply data to the TSF, receive data from the TSF and invoke services from the TSF.

- CP-London-2008-GE-2007-0074

CEM, SFR-related interfaces of SFR-supporting modules:

ADV_TDS.4.8C states:

The design shall describe each SFR-enforcing and SFR-supporting module in terms of its SFR-related interfaces, return values from those interfaces, interaction with and called interfaces to other modules.

It is unclear what the SFR-related interfaces of SFR-supporting modules are. By definition SFR-supporting modules do not implement any aspect of an SFR. Paragraph 864 of the CEM 3.1R2 states:

The SFR-related interfaces of a module are those interfaces used by other modules as a means to invoke the SFR-related operations provided, and to provide inputs to or receive outputs from the module. [...] Inter-module interfaces that are not SFR-related need not be specified or described, since they are not a factor in testing.

Again, since by definition a SFR-supporting module does not have SFR-related operations, one could deduce that no interfaces of SFR-supporting modules need to be described for ADV_FSP.4. This would contradict the explicit inclusion of SFR-supporting modules in requirement ADV_TDS.4.8C.

- CP-London-2008-GE-2007-0075

CEM, ADV_TDS.4-2:

ADV_TDS.4 introduces a new requirement (ADV_TDS.4.4C) for a semiformal description of each subsystem. The new evaluator work unit to examine this is work unit ADV_TDS.4-2, which is associated with ADV_TDS.4.1C.

Proposal: Move work unit ADV_TDS.4-2 to be a work unit associated with ADV_TDS.4.4C.

- CP-London-2008-GE-2007-0076

CEM, inconsistent use of architectural description:

Throughout the CC 3.1R2 the term "architectural description" is used inconsistently. CEM 8.5.5.3.2 describes the "architectural description" as a part of the ETR where the evaluator reports the high level description of the TOE and its major components. Paragraph 537 and 546 of CEM V3.1 mention the term "architectural description" but mean the TOE security architecture documentation. Paragraph 709 of CEM 3.1R2 mentions the architectural description as an input document for ADV_INT (probably meaning the TSF internals description). In work unit ADV_TDS.4-3 the architectural description is mentioned as other

evidence that could provide input to the work unit, meaning obviously the TOE security architecture documentation.

- CP-London-2008-GE-2007-0077

Part 3, Removal of ADV_SPM.1.5C, since it is redundant to ADV_SPM.1.4C.

- CP-London-2008-GE-2007-0078

Part 3: A normative definition of PP evaluation assurance packages was missing.

- CP-London-2008-GE-2008-0001

Part 2, Correction of FDP_ACF.1.4:

In the definition of FDP_ACF.1.4 the words "following additional rules" are missing.

- CP-London-2008-GE-ATE_DPT

The package EAL4 needs to include ATE_DPT.1 instead of ATE_DPT.2 for compatibility reasons. The text for ATE_DPT.1 needs clarification for this.